Tech & Snack: FortiProxy

Laurent Cohn, Systems Engineer

October 26th, 2022

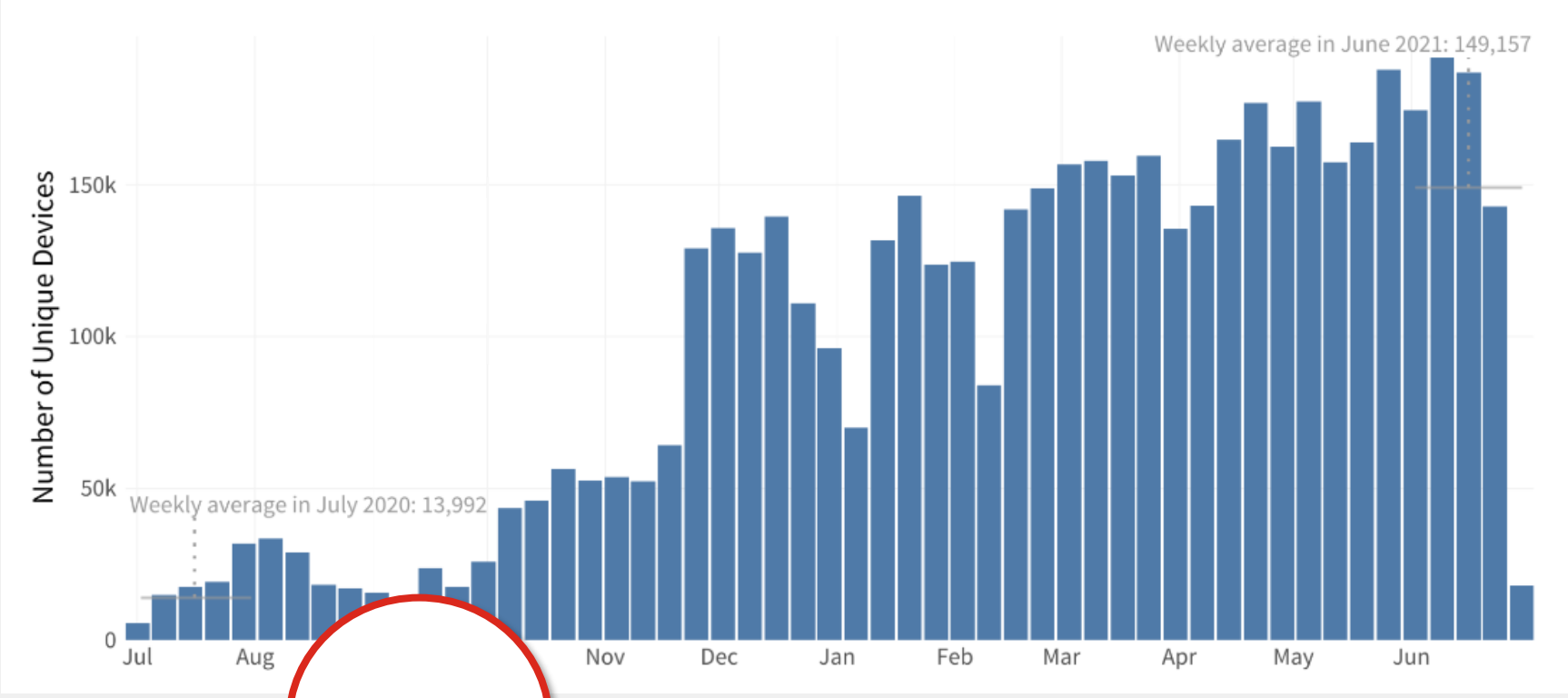
Agenda

- A concerning development in the Cybersecurity World
- FortiProxy
- FortiProxy as a Service
- FortiProxy Tips & Tricks
- Training & Licensing

A concerning development in the Cybersecurity World…

Global Surge in Ransomware and Malware Attacks

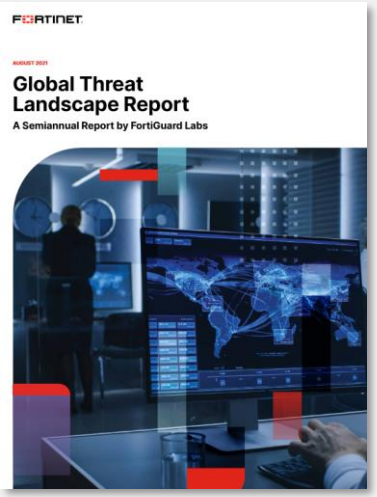
Hackers taking advantage of the situation..



10.7x **increase of ransomware within one year**

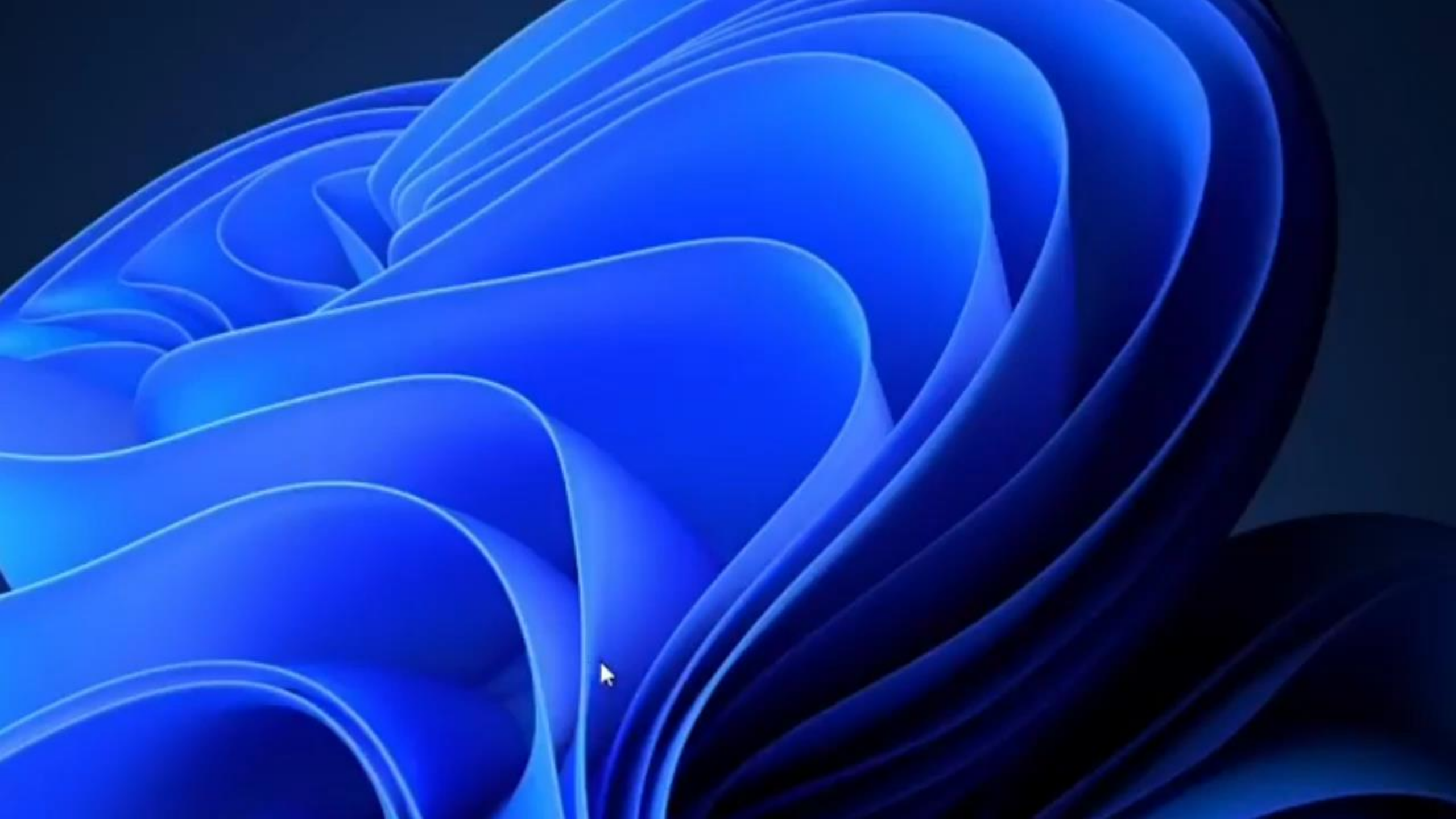
Remote workforce remains target

Onslaught of ransomware continues

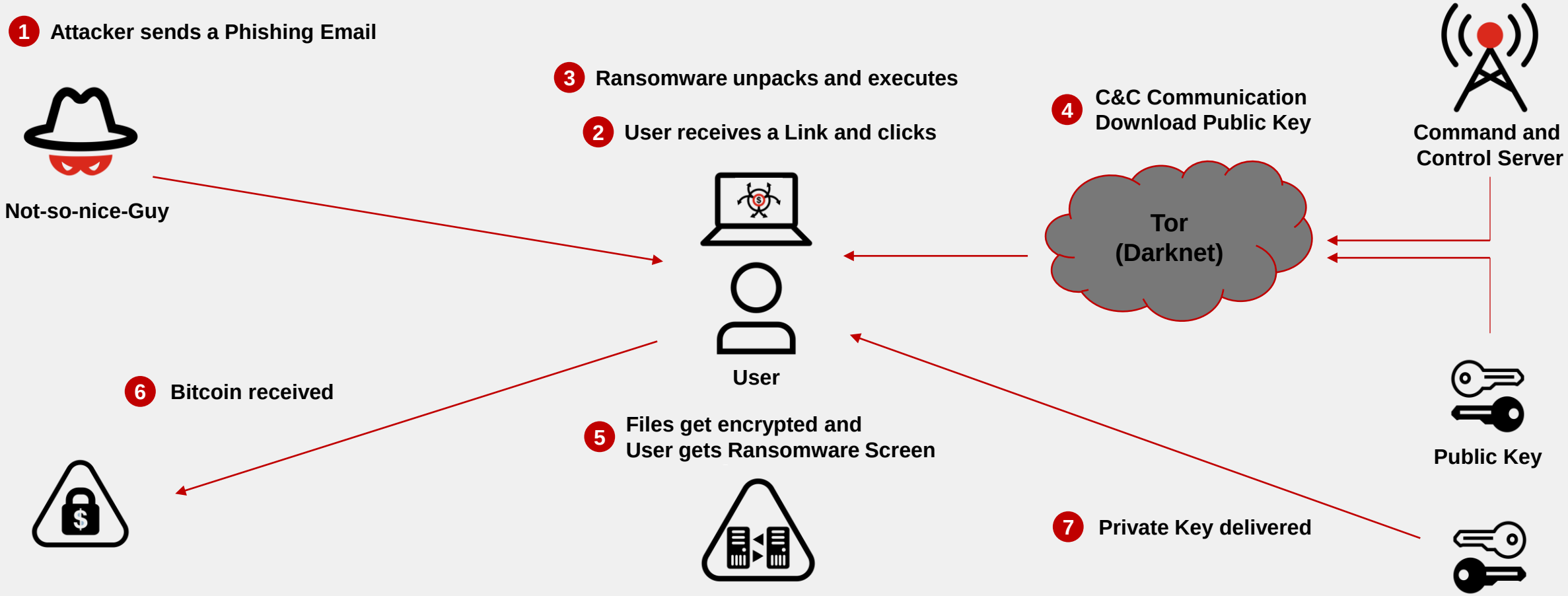


Ransomware “Offerings” in the Darknet

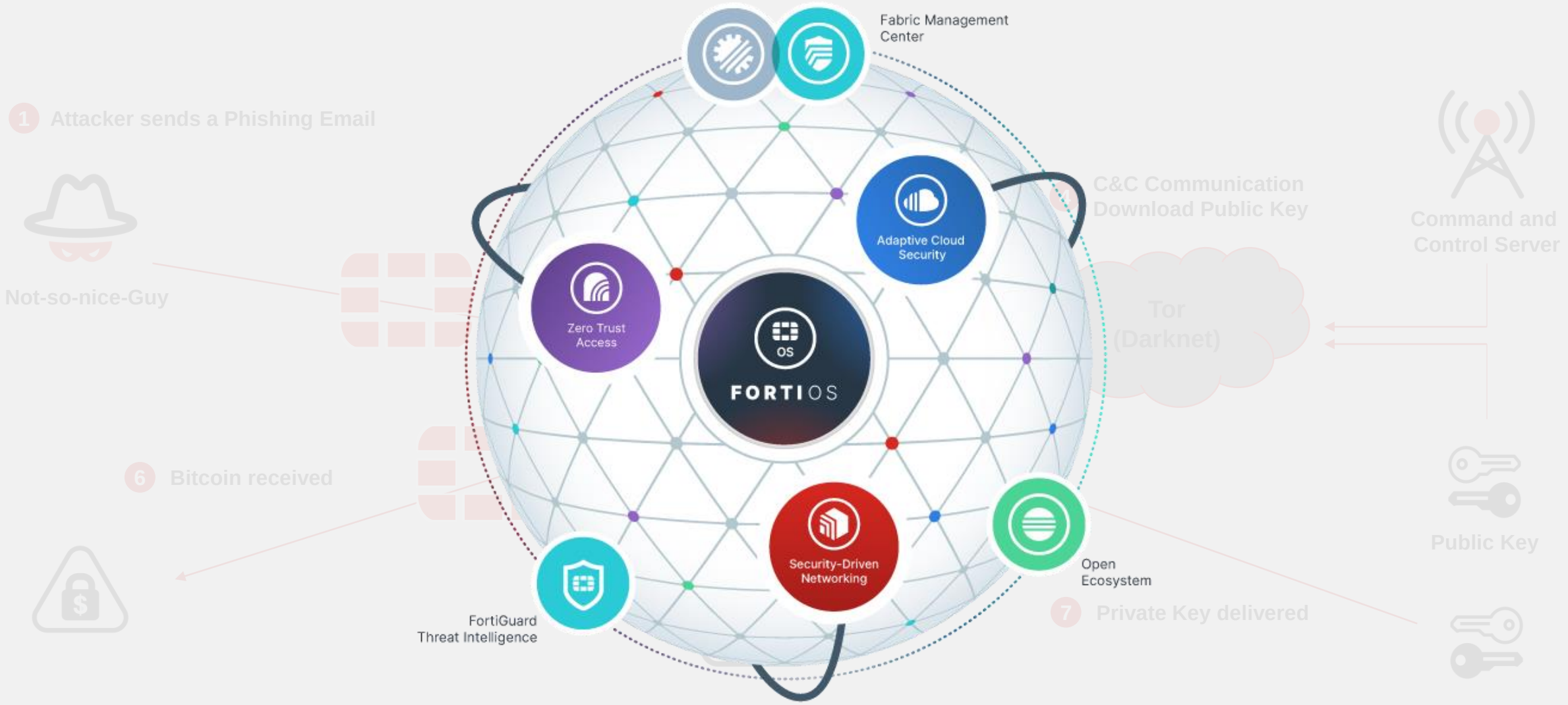
Ransomware as a Service and more…



How does Ransomware work?



How does Ransomware work?



Advanced Web Based Attacks

- Email (92.3%) and **Web (6.3%)** are the two main primary vectors for malware entering an organization.
- 4% of people will click on a phishing email which is often used to gain a foothold in the network via malware or credential phishing.
- Malware laden scripts and adverts mean malware can show up on the most popular and trusted websites

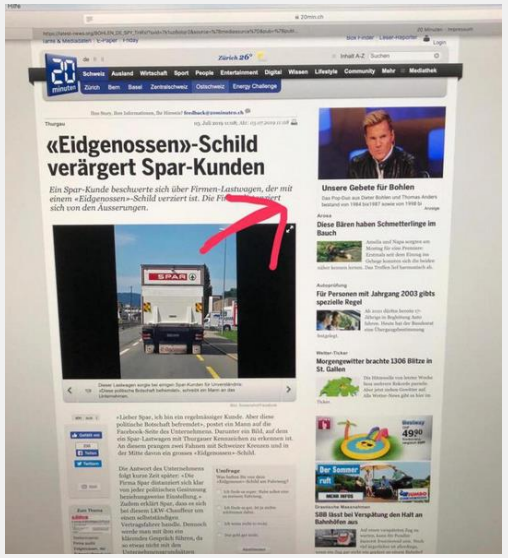
20minuten.ch erneut Ziel von Malware-Attacke

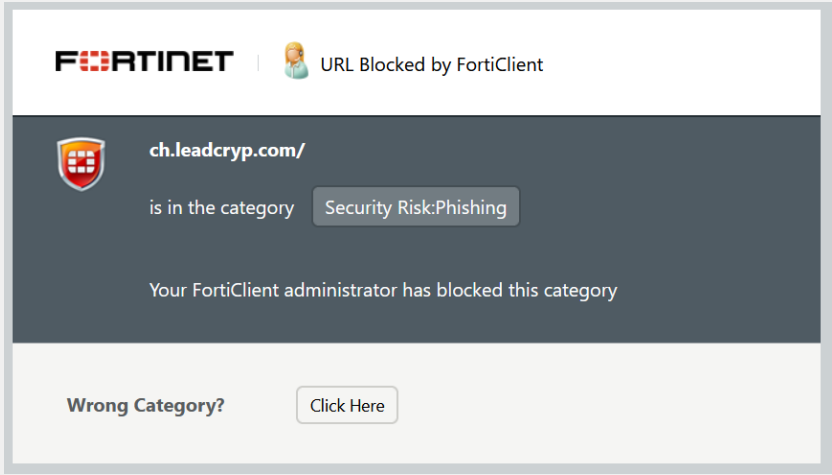
Am Montag wurde über 20min.ch erneut Malware verteilt. Schuld war ein verseuchtes Netzwerk eines Werbeanbieters. Die Anzeige wurde blockiert.

Nach aktuellem Wissensstand sind nur Windows-Systeme betroffen. (Foto: Flickr / Andrew Writer)

Source: https://www.20min.ch/digital/news/story/20minuten-ch-erneut-Ziel-von-Malware-Attacke-15457508

Advanced Web Based Attacks

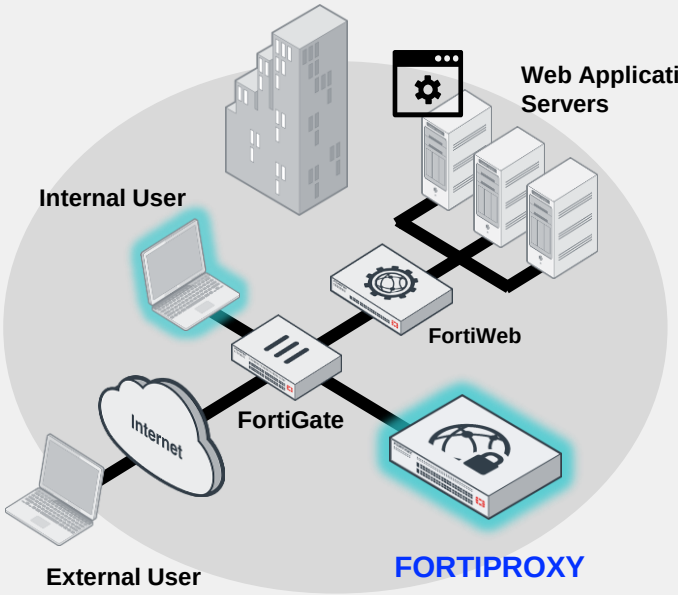




https://www.20min.ch/story/bitcoin-betrueger-zocken-mit-berset-masche-schweizer-ab-247011714310

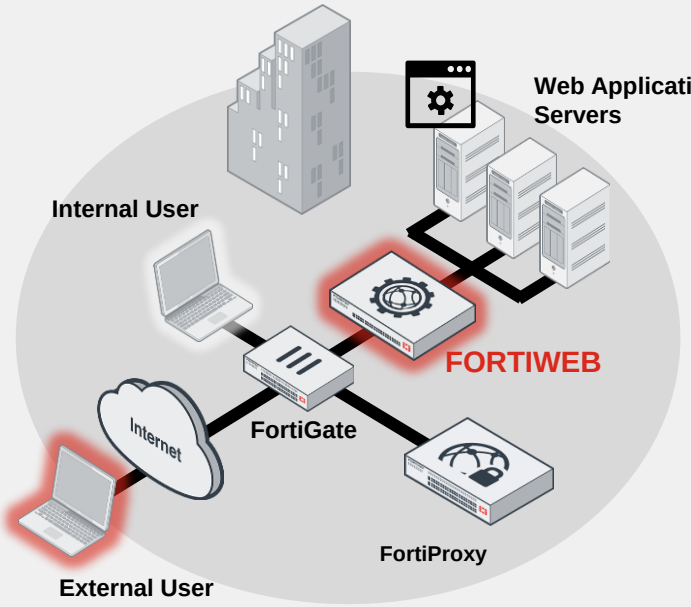
SWG != WAF != NGFW

Protects Users from Internet Threats



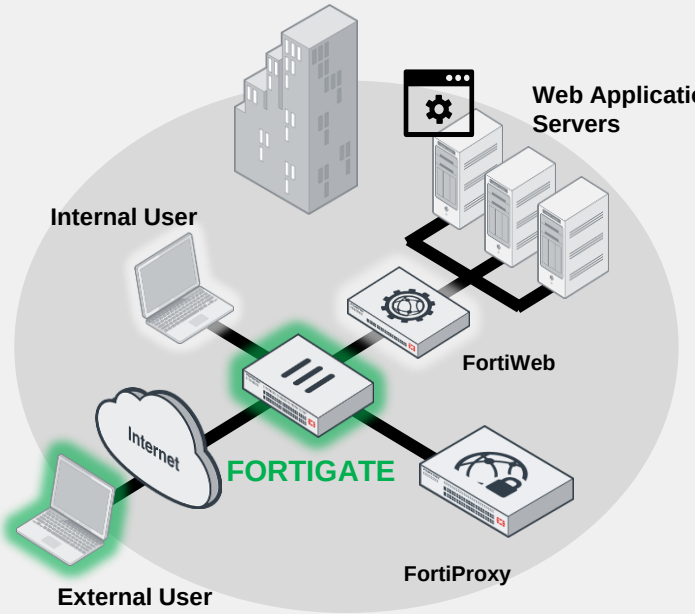
- Proxy Mode Application
- Protect users from internet-borne threats with:
  - URL filtering
  - Anti-malware protection
  - IPS
  - DLP
  - Application control capabilities
  - SSL Inspection
  - Optimizing user experience

Protects Internal Web Application Servers



- Only HTTP/S traffic
- Protect web applications against a variety of attacks
- Protection from the OWASP Top Ten application attacks

Protects Internal Network/Application

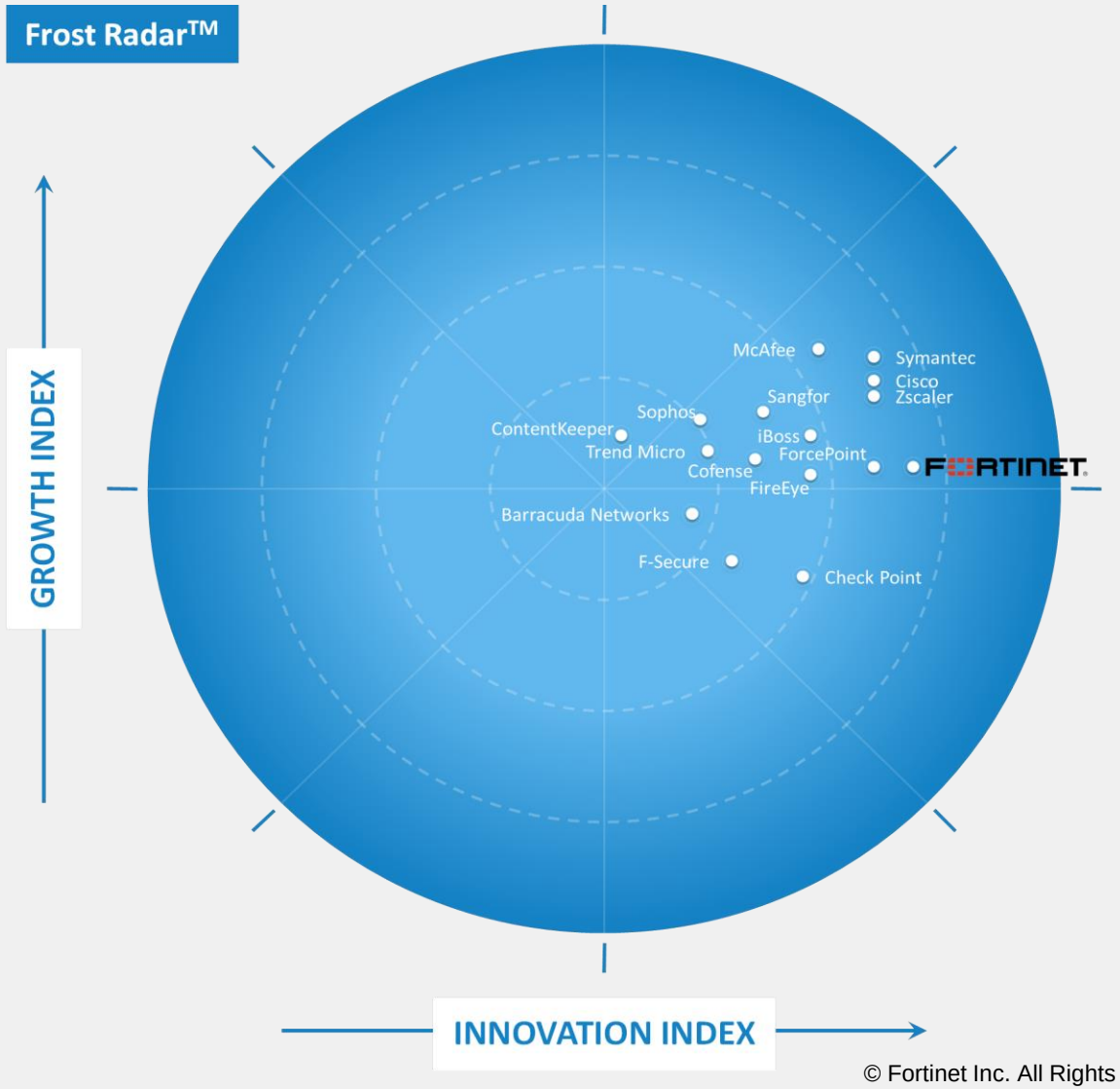


- Network Segmentation
- Flow/Proxy Traffic
- Protect against External/Internal threats with:
  - Anti-Virus and Malware
  - IPS
  - SSL Inspection/Offloading
  - Application rules
  - …

FortiProxy

FROST RADAR™: Global Web Security Market, 2020

FortiProxy positioned as most innovative Solution



Seamless Integration with Fortinet Security Fabric

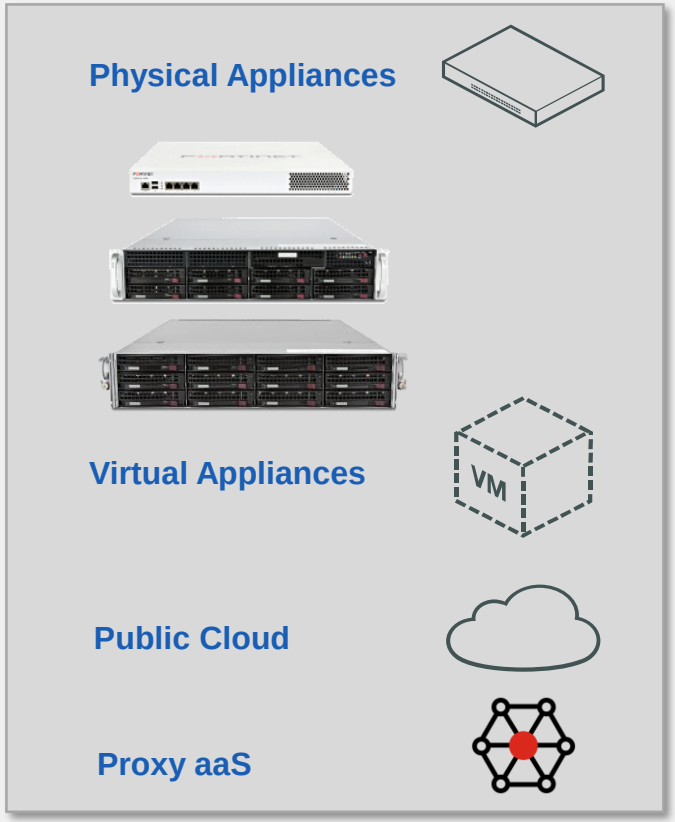
Powered by Marketing leading Threat Intelligence, FortiGuard Labs

High Growth Rate in the market

Source: https://store.frost.com/frost-radartm-global-web-security-market-2020.html

FortiProxy Secure Web Gateway

- High Performance and Scalability Proxy
- Dedicated Secure Web Gateway Solution
- Multi-Layered Detection to prevent threats
- Zero Trust Web Browsing
- Authenticated Web Application Control
- Wan Optimization and Advanced Caching
- Data Loss Prevention
- Centralized Management
- Pay As You Grow License



SSL INSPECTION

- Powerful hardware
- Removes blind spots in encrypted traffic
- Multiple inspection methods

MULTI-LAYERED PROTECTION

- Integration with proven FortiGuard Threat Intelligence
- Integration with FortiSandbox

AUTHENTICATED ACCESS

- Granular application control policies
- Activity monitoring
- Restricts access to social websites using user or group identity

Use-Case #1 - On-Prem SWG Services

Method supported

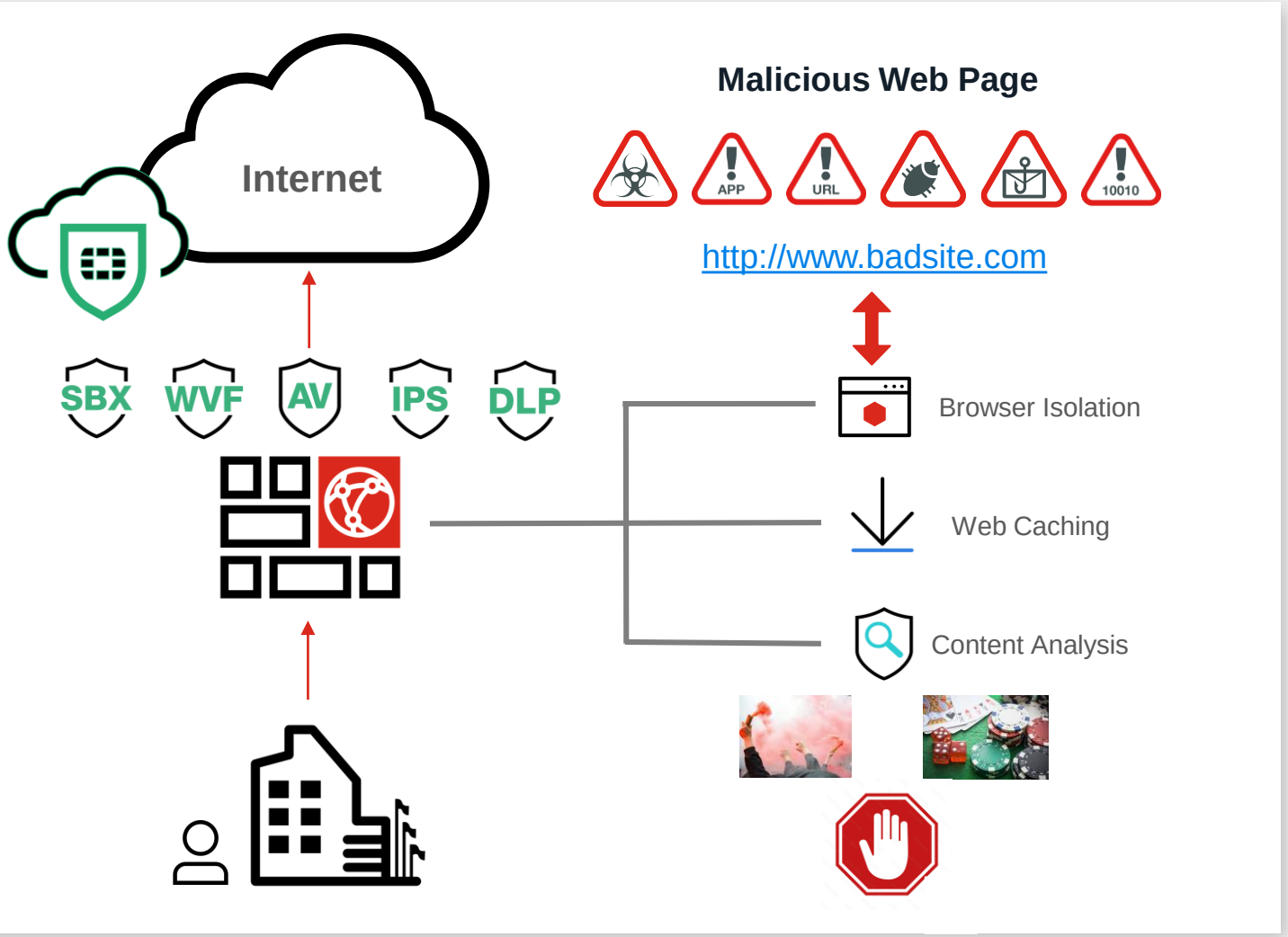
Explicit Proxy, Transparent, PBR and WCCP

How we solve it

- FortiProxy employs multiple FortiGuard services to protect users against the latest web threats and to enforce compliance.
- Integration with FortiGuard Threat Intelligence Service
- Advanced Web Caching Solution

Benefits

- Advanced SWG Services
- Full Visibility



Use-Case #2 - Hybrid Cloud Solution

Method supported

On-prem HW/VM, Agent-based, Agentless

How we solve it

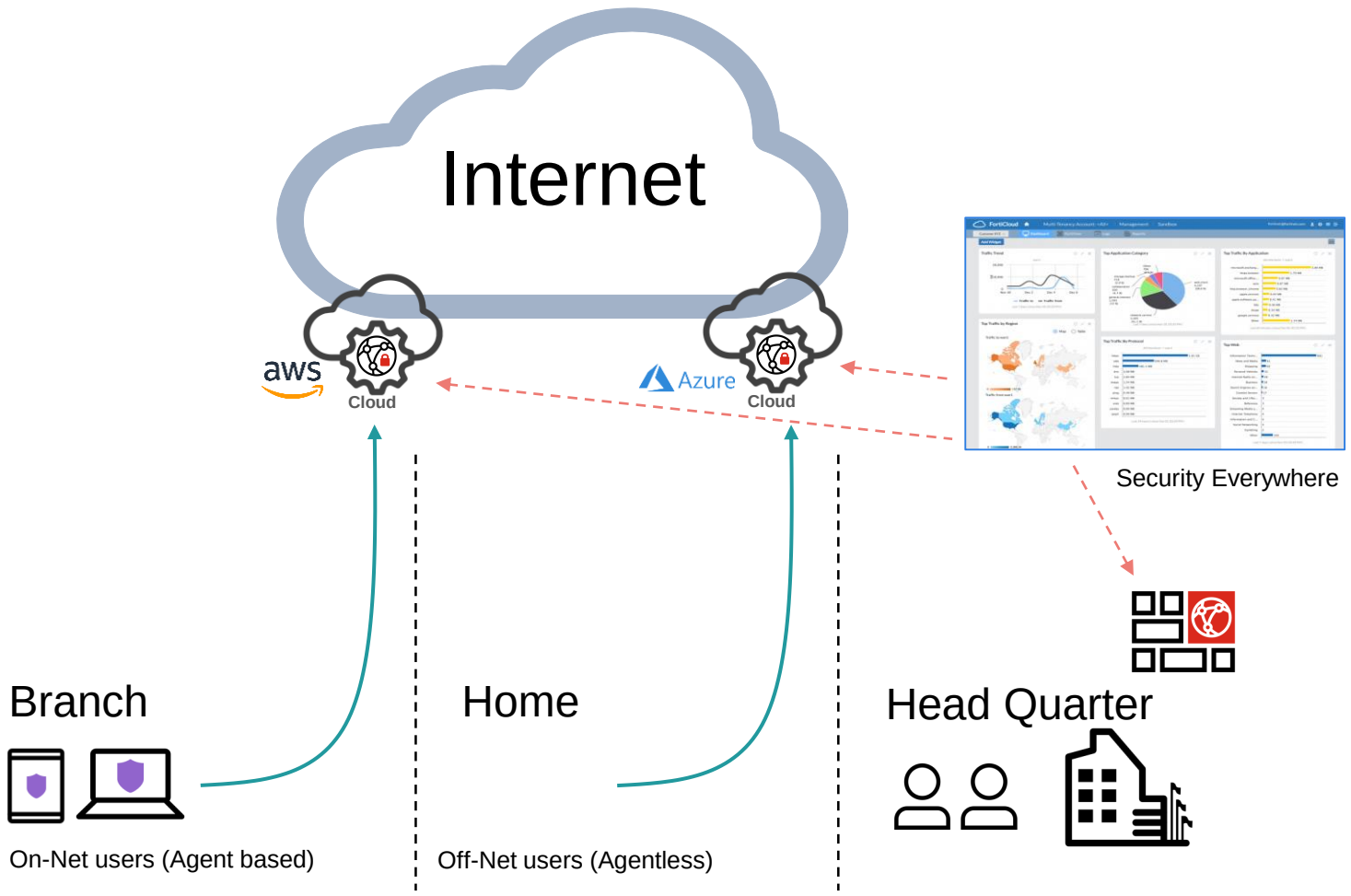
- License Sharing
- Explicit Proxy with PAC File hosting support or SSL-VPN
- GSLB for Geo location LB - possible integration

Benefits

- Auto scaling
- Full Visibility
- Consistent Security Across all users

Deployment

- Fast on-boarding via cloud template (needed supporting cloud-init for configuration)
- Provisioning FortiProxy on GCP -
- https://github.com/40net-cloud/fortinet-gcp-solutions/tree/master/FortiProxy/dm



Use-Case #3 - SWGaaS for MSSP (VDOMs – v7.2)

Method supported

On-prem HW/VM, Agent-based, Agentless

How we solve it

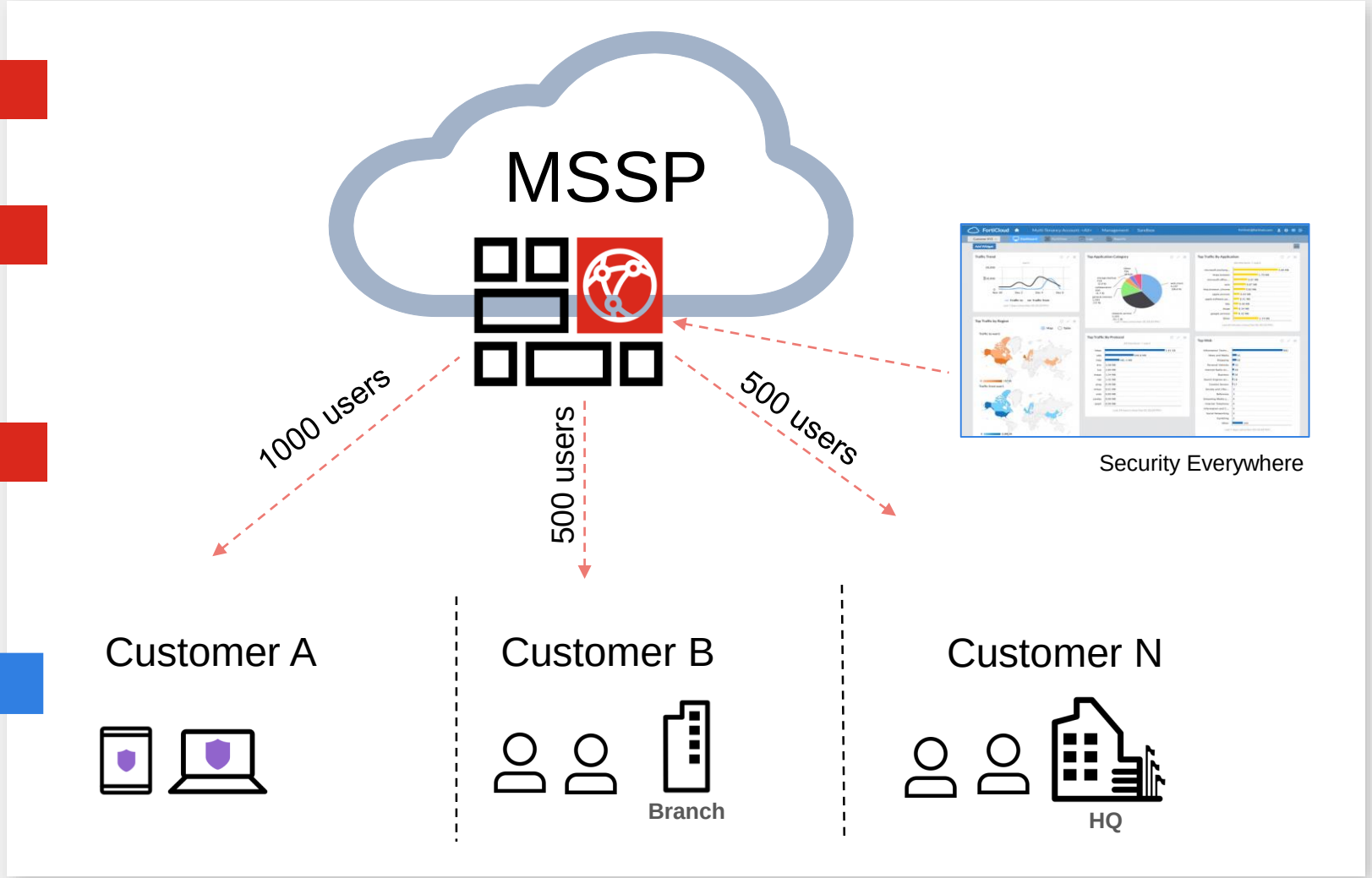
- License sharing per customer
- Explicit Proxy with PAC File hosting support or SSL-VPN

Benefits

- SWGaaS for MSSP customers
- Full Segregation
- Full Visibility

Deployment and Requirements

- Full API and Terraform support
- Single pane of glass (FMG and FAZ)
- Solution guide and docs
- AT&T Secure Web Gateway MSSP as an example (https://cybersecurity.att.com/products/secure-web-gateway)



Fabric Management Center

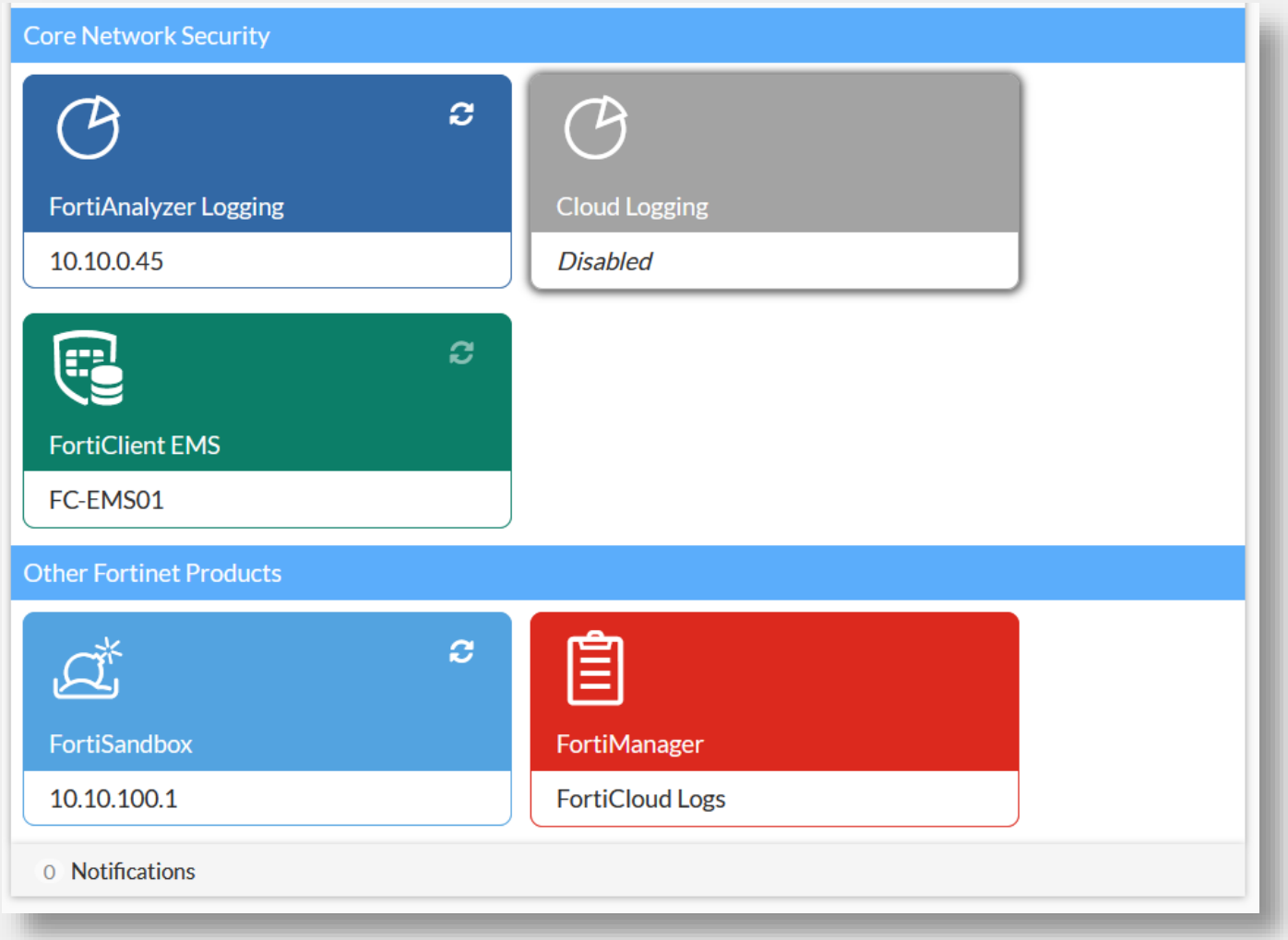
New Security Fabric Page for FortiProxy

Integrated with all Fortinet Family for better Security:

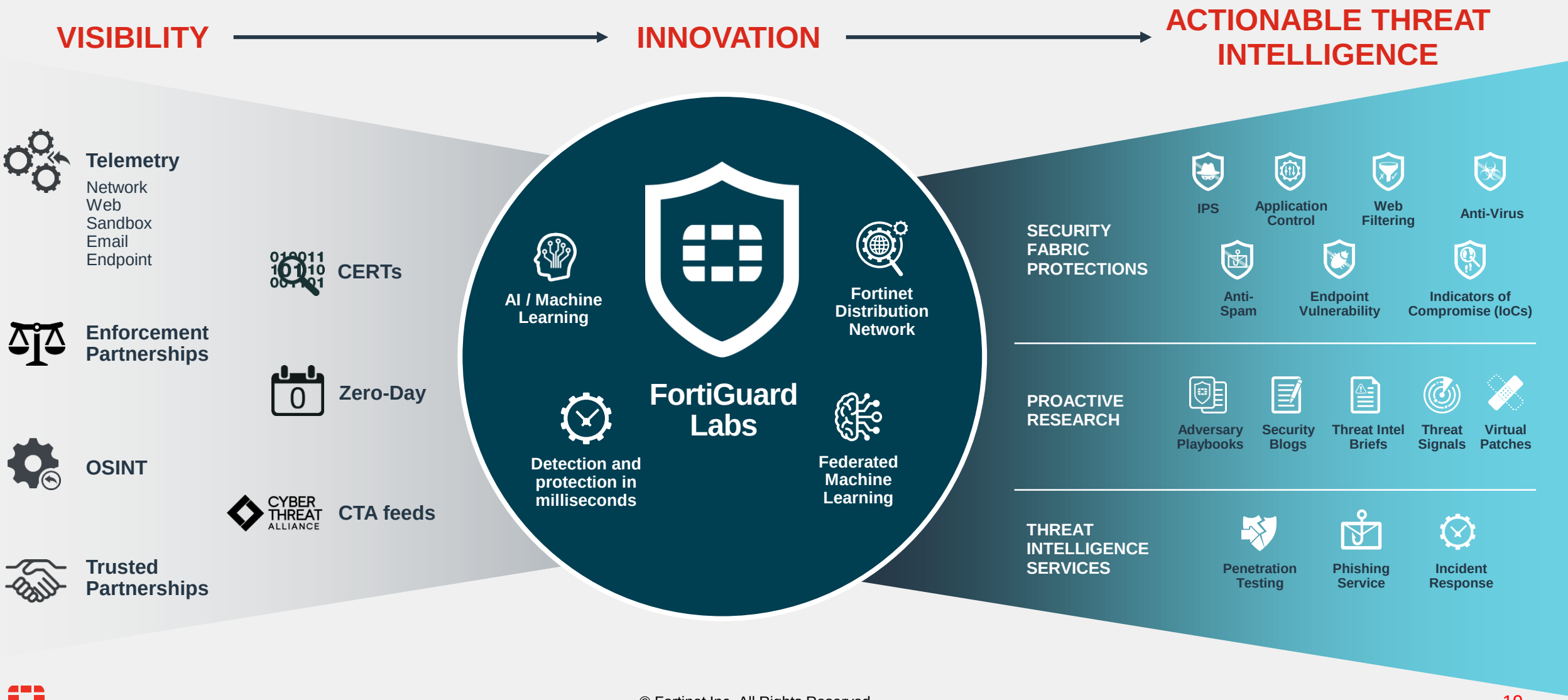
- FortiAnalyzer
- FortiSandbox
- FortiClient
- FortiCloud
- FortiManager

3rd party Integration:

- Cloud providers (AWS, Azure, GCP)
- Private SDN
- End Point Solution / Identity
- External Threat Feeds



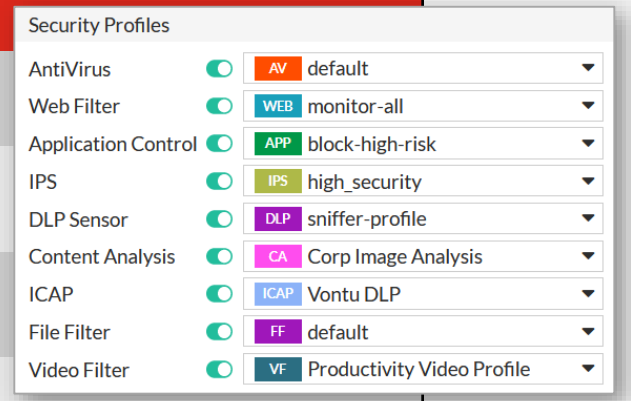
FortiGuard Labs Threat Intelligence



FortiProxy Threat Intelligence from FortiGuard

New Features in Version 7.x

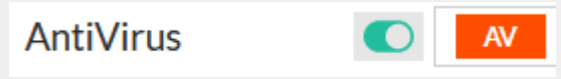
Threat Intel Service	Type	Usage
Antivirus	Signature DB, AV Engine	AV Profile
Outbreak Prevention NEW	Cloud-based Query	AV Profile
FortiProxy Cloud Sandbox	Cloud-based Hosted Service	AV Profile
Content Disarm & Reconstruct NEW	Feature	AV Profile
Botnet IP and Domains	IP, domain list	IPS Profile, DNS Profile
IPS	Signature DB, IPS Engine	IPS Profile
Web Filtering	Cloud-based Query	Web Filter Profile, DNS Profile
Video Filtering NEW	Cloud-based Query	Video Filter Profile
URL certificate blacklist	fingerprint-based certificate list	SSL/SSH Profile
Application Control	Signature DB, CASB	Application Control Profile

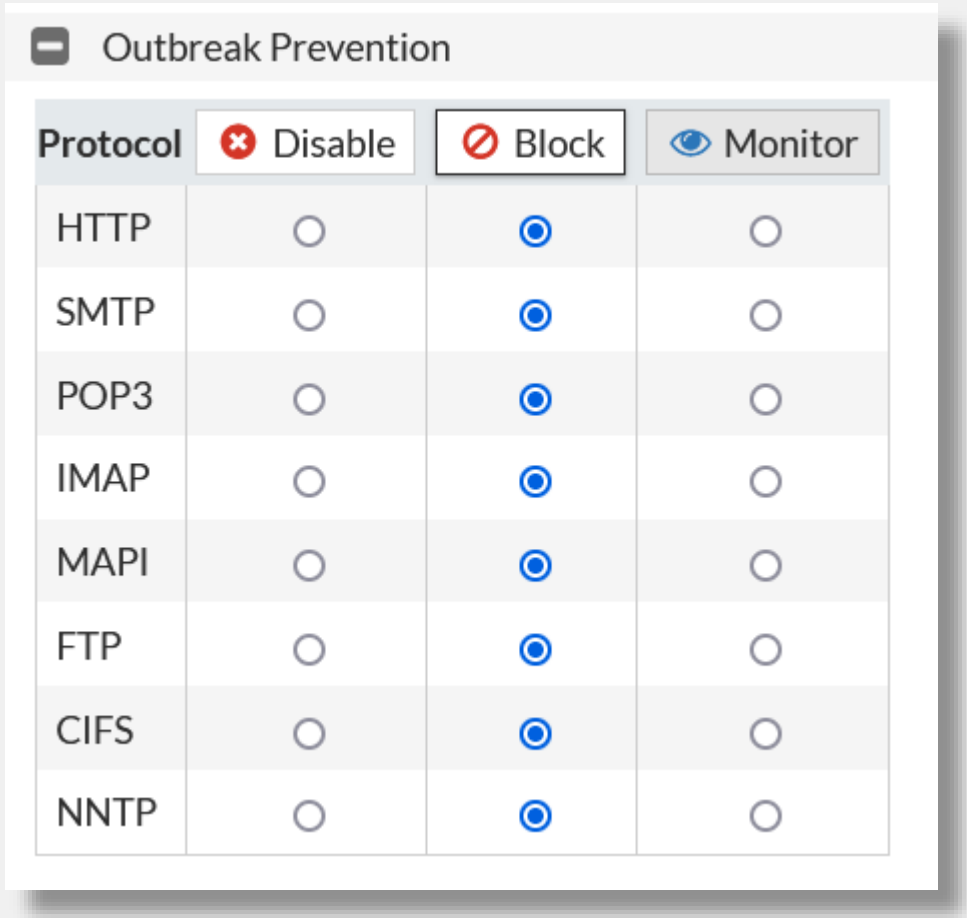


FortiProxy Security Services

FortiGuard Outbreak Prevention for antivirus

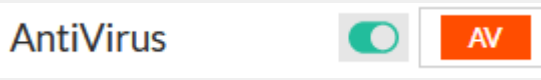
- FortiGuard Outbreak Prevention allows the FortiProxy antivirus database to be subsidized with **third-party malware hash signatures** curated by FortiGuard to detect zero-day malware in a collaborative approach.
- The **hash signatures** are obtained from external sources such as VirusTotal, Symantec, Kaspersky, and other third-party websites and services.
- This feature provides the mechanism for **real-time antivirus query** to FortiGuard to stop malware threats discovered between signature updates before they can spread throughout an organization.





FortiProxy Security Services

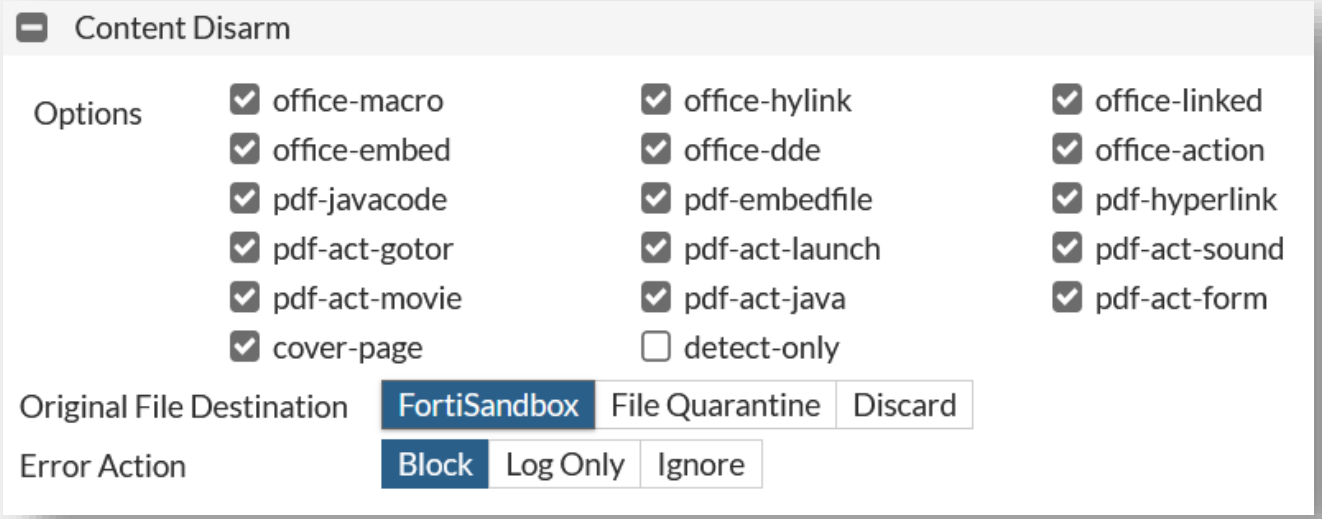
Content Disarm and Reconstruction for antivirus (CDR)



- Content Disarm and Reconstruction (CDR) allows the FortiProxy to sanitize Microsoft documents and PDF (disarm) by removing active content such as hyperlinks, embedded media, javascript, macros, etc. from the office document files without affecting the integrity of its textual content (reconstruction).
- This feature allows network admins to protect their users from malicious office document files.

Notes:

- CDR can **only** be performed on Microsoft Office Document and PDF files.
- CDR supported on HTTP, SMTP, POP3, IMAP



FortiProxy Security Services

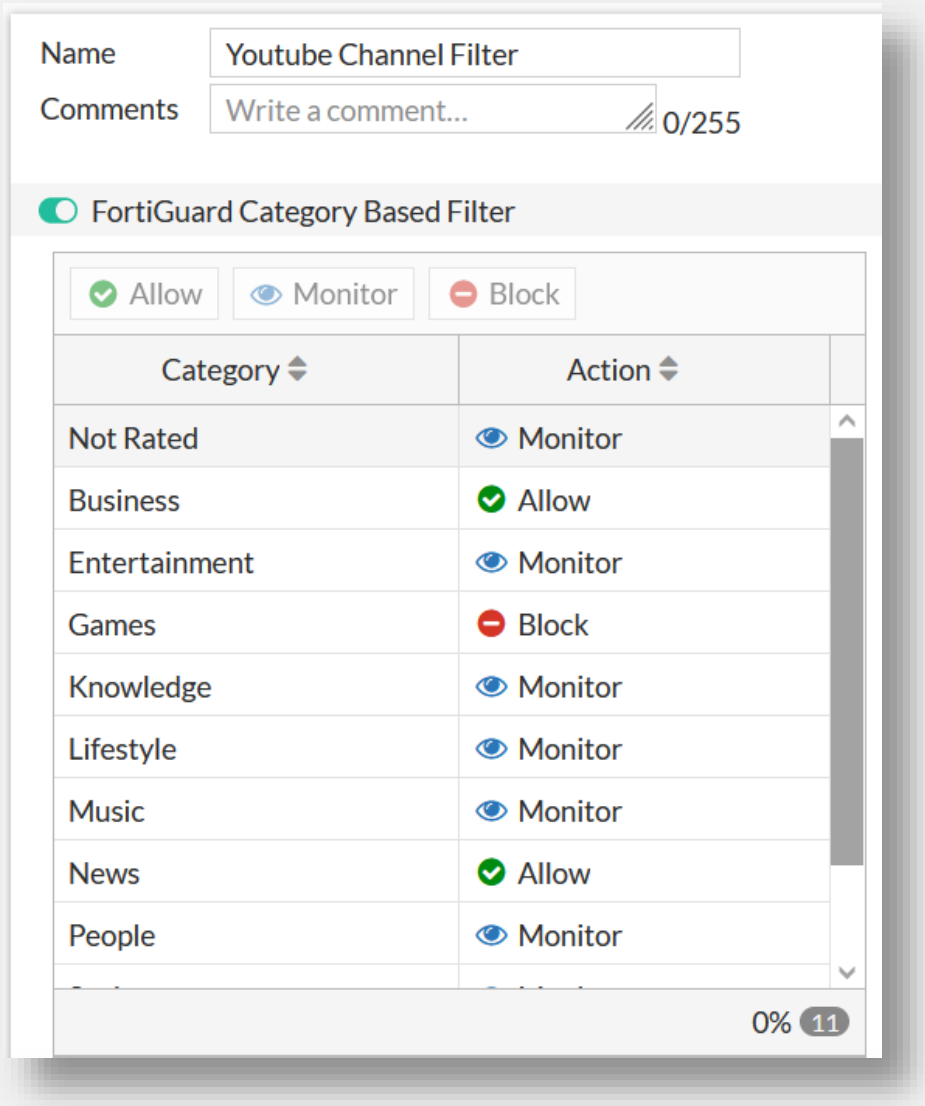
FortiGuard Video Filtering Service

Add FortiGuard service that provides category rating for videos under new video filter profile panel

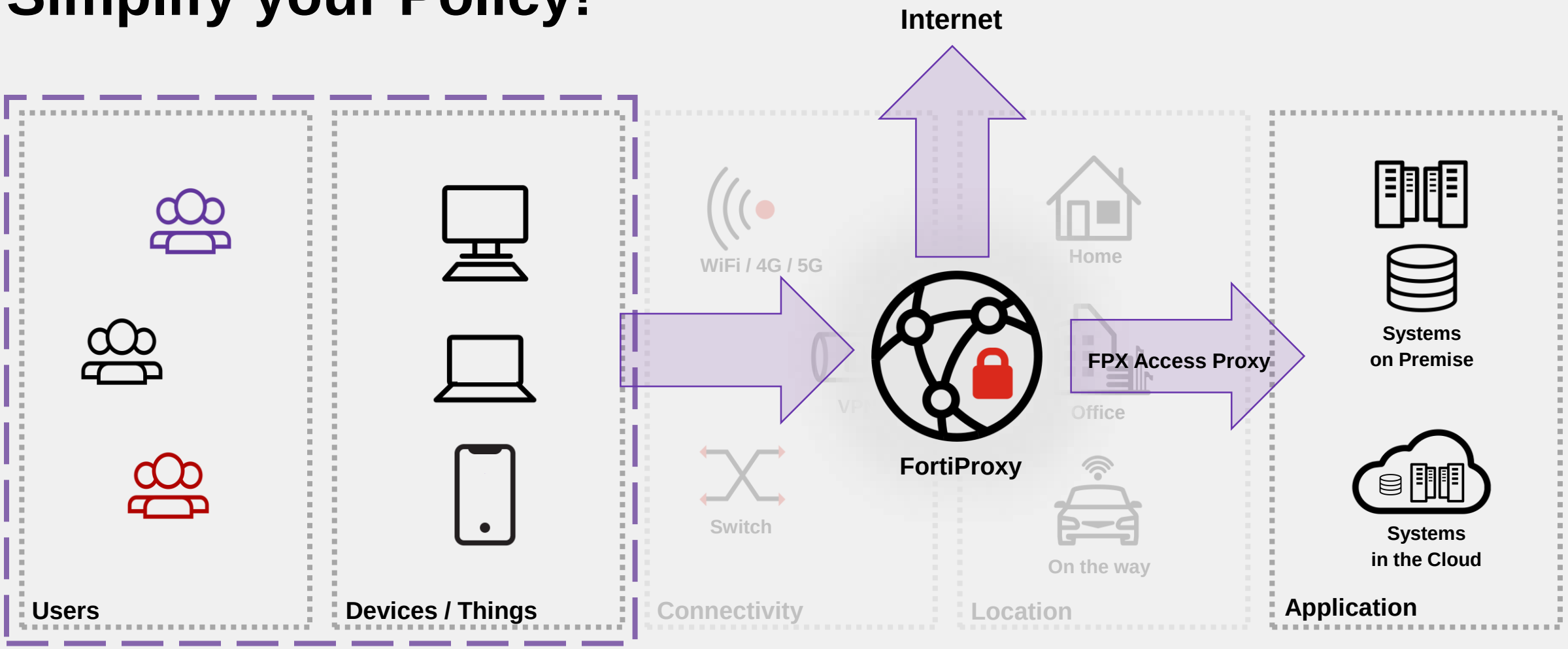
- Support Video Filtering based categories

  (Games, Music, News…)

- Support YouTube, Vimeo and Daily Motion



Simplify your Policy!



ZTNA with FortiClient / FortiEMS / FortiNAC
FortiAuthenticator / FortiEDR / ...

SD-WAN / FortiAP / FortiSwitch / FortiGate /
FortiExtender / ...

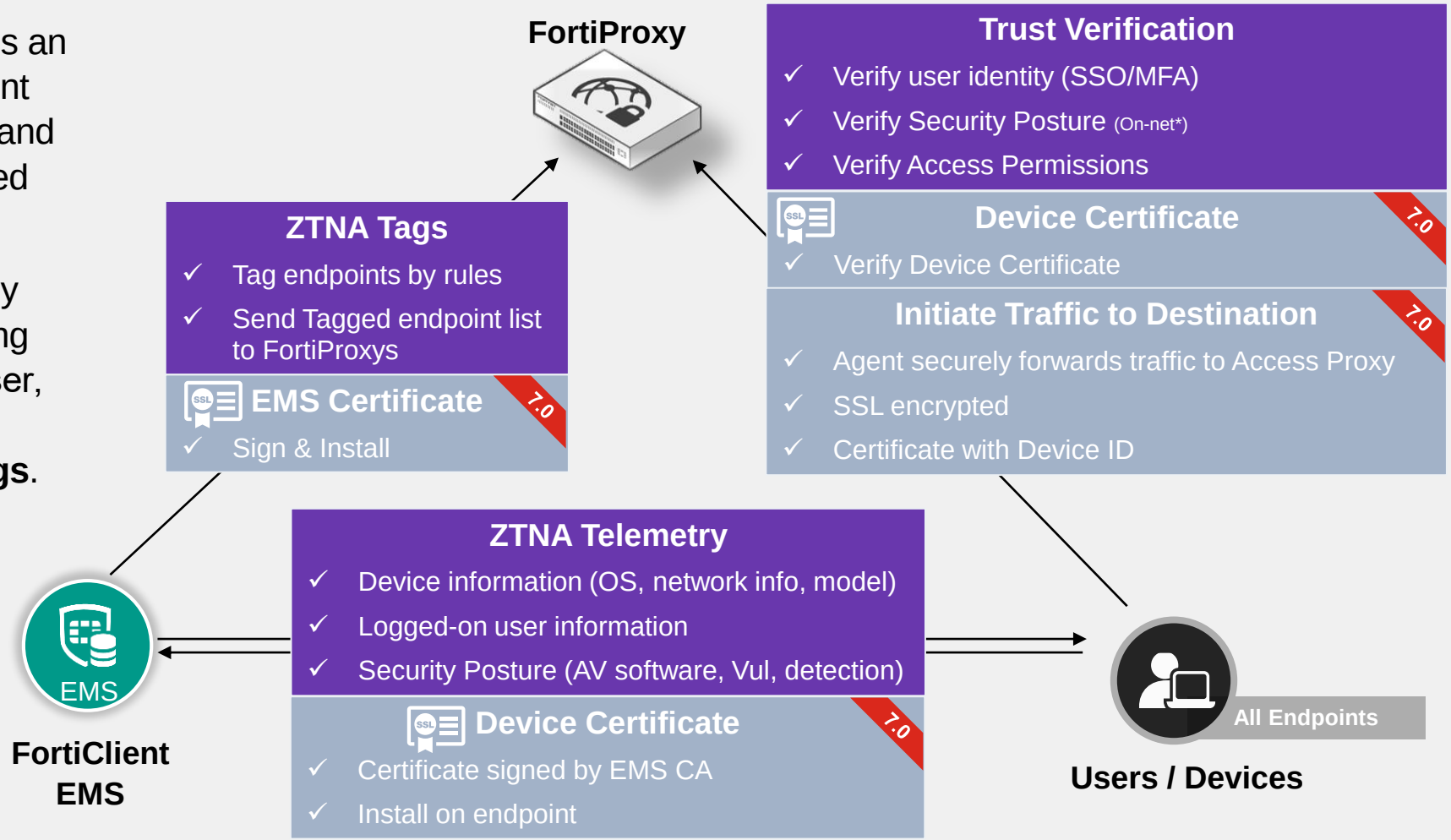
Zero-Trust Network Access

New Zero Trust Solution

Zero Trust Network Access (ZTNA) is an access control method that uses client device identification, authentication, and **Zero Trust tags** to provide role-based application access.

Access to applications is granted only after device verification, authenticating the user's identity, authorizing the user, and then performing context based posture checks using **Zero Trust tags**.

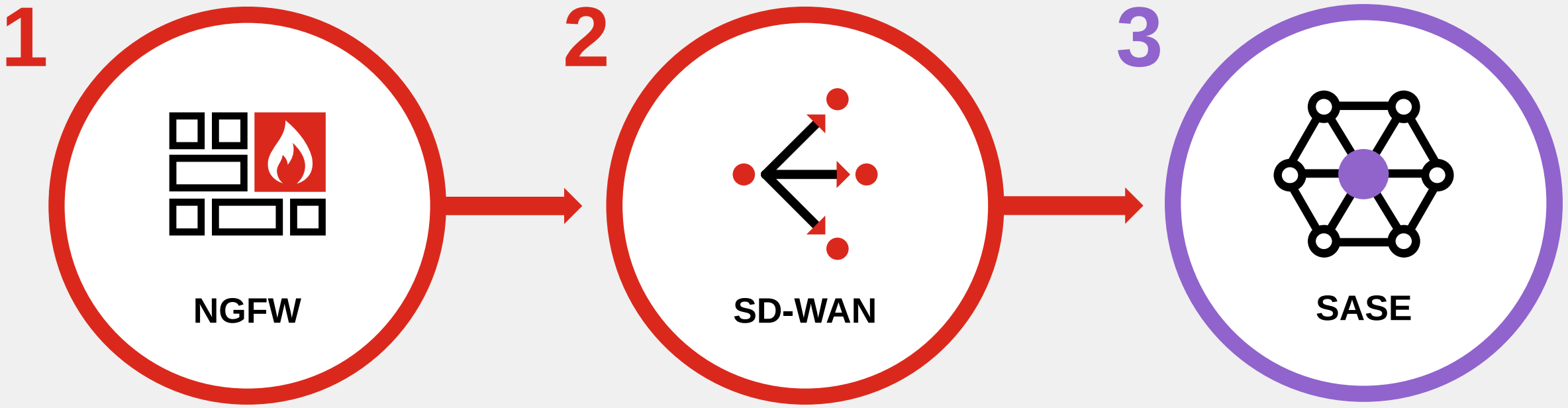
- **HTTPS access proxy with FortiClient as ZTNA agent**
- Support trust verification with certificate-based authentication



FortiProxy as a Service

Pragmatic Journey to SASE

With Fortinet's convergence of security & networking everywhere

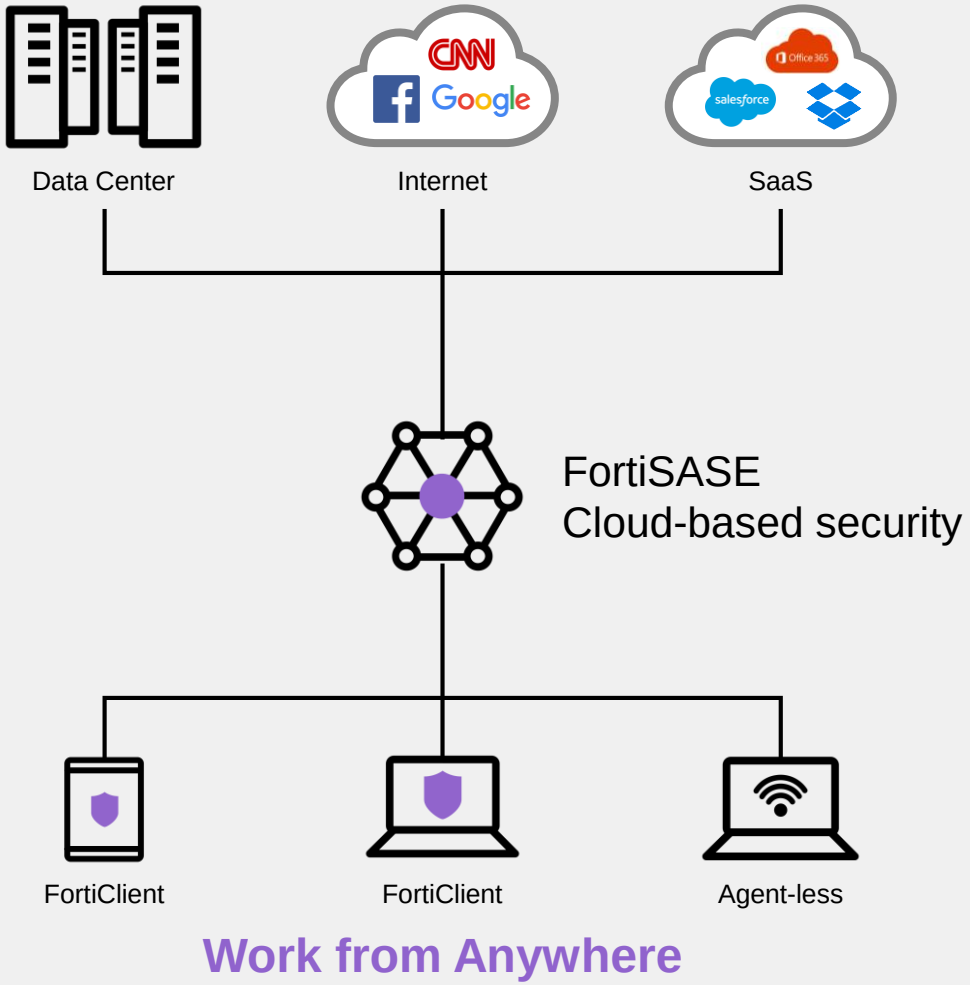


Secure Edge Connectivity

Optimize Application Experience

Secure Remote Users

Securing Remote Users with FortiSASE

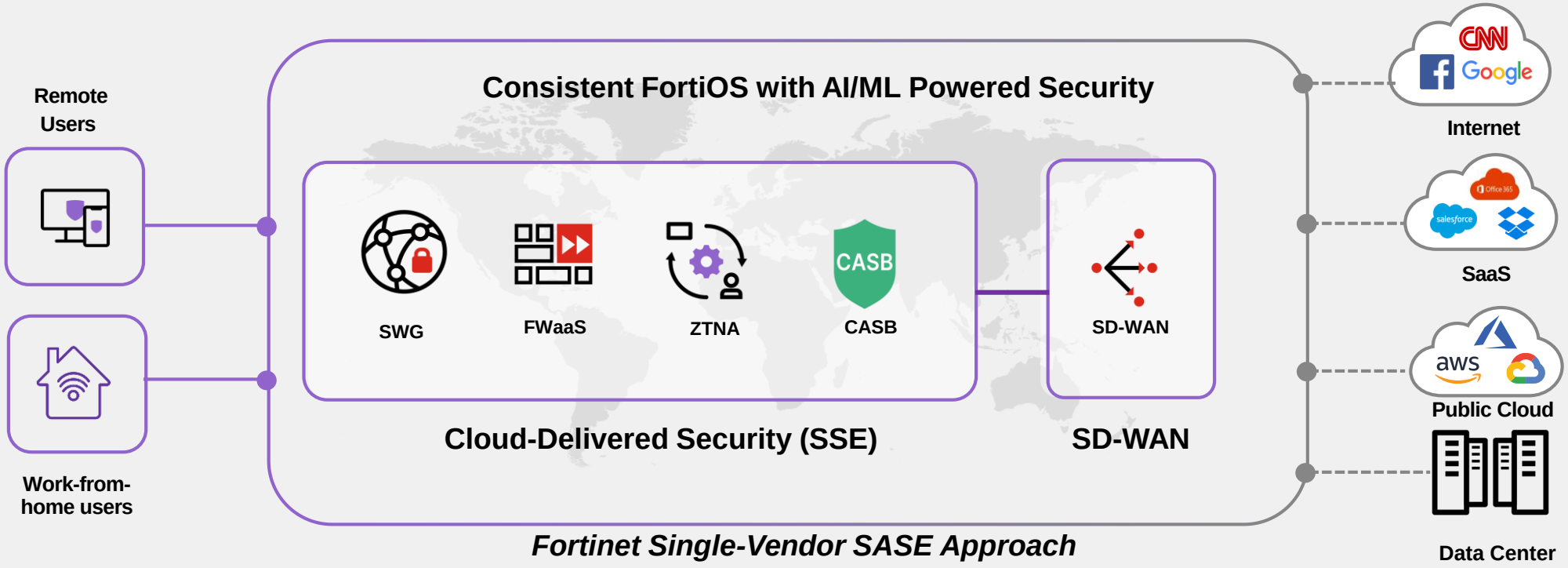


Secure Internet Access for Safe browsing

Secure Private Access to Corporate Apps

Secure SaaS Access to Cloud apps

FortiSASE: Cloud-Delivered Security & Networking



Secure Hybrid Workforce with Consistent Security

Superior User Experience with Operational Efficiency

Shift from CAPEX to OPEX Based model

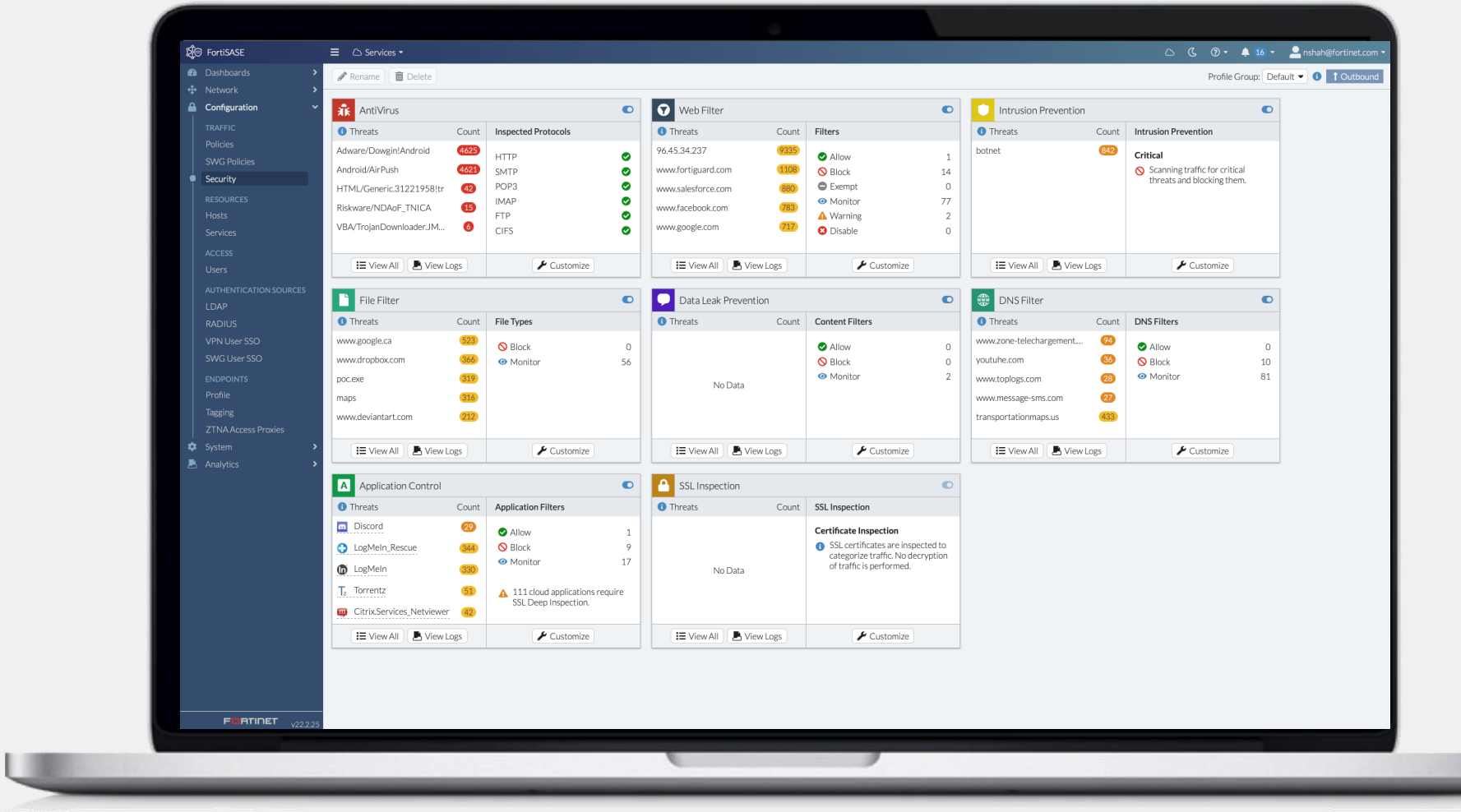
Customizable Dashboard for Cloud-Delivered Security

CAPABILITIES

- FortiGuard Security Services
- IPS, Sand-box
- URL and DNS Filtering
- Anti-Malware, DLP
- SSL Inspection

BENEFIT

- Better Threat Protection
- Improved User Experience



FortiProxy Tips & Tricks

From Bluecoat to Fortinet

ProxySG	Content Analysis	Advanced Secure Gateway	Management Center MC	Reporter RP	SSLv
Physical ***Virtual*** ***Cloud BYOL***	***Physical*** ***Virtual*** ***Cloud BYOL***	***Physical***	***Physical*** ***Virtual***	***Physical*** ***Virtual***	***Physical*** ***Virtual***
Proxy SG 300 Proxy SG S200 Proxy SG S400 Proxy SG S500	CAS-S200 CAS-S400 CAS-S500	ASG S200 ASG S400 ASG S500	MC S400	RP S500	SV1800 SV2800 SV3800
Proxy SG-VA	CAS-V100		MC-V10	RP-V50/100/200	SV-VA-C8

+BCIS Bluecoat Standard or Advanced Intelligence Services | CASB Audit AppFeed

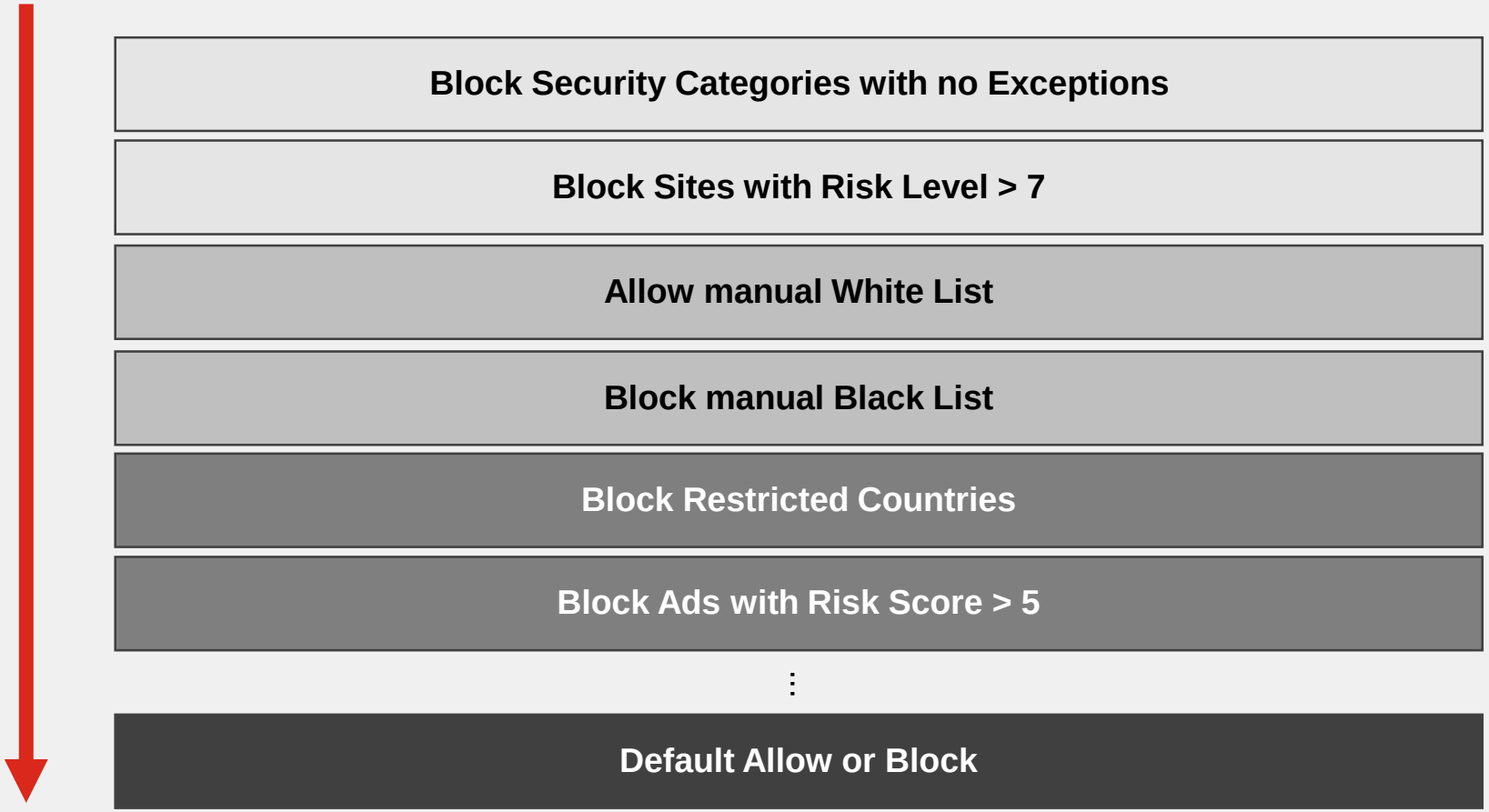
FortiProxy | FortiSandbox | FortiProxy + FortiSandbox | FortiManager | FortiAnalyzer | «CP9»







Proxy Policy - Migration



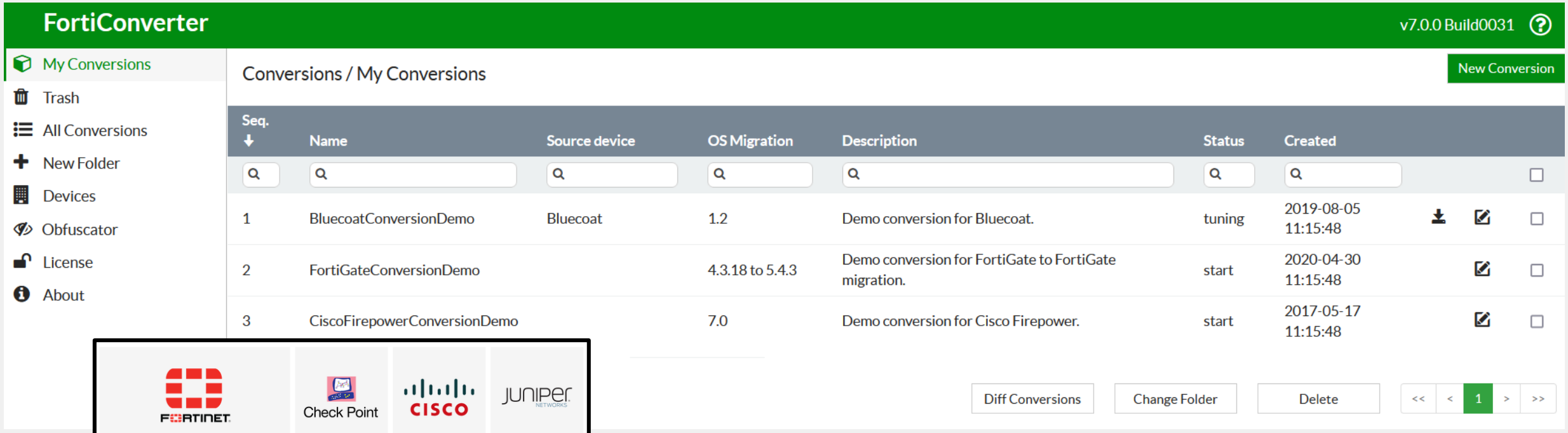
Key Message:

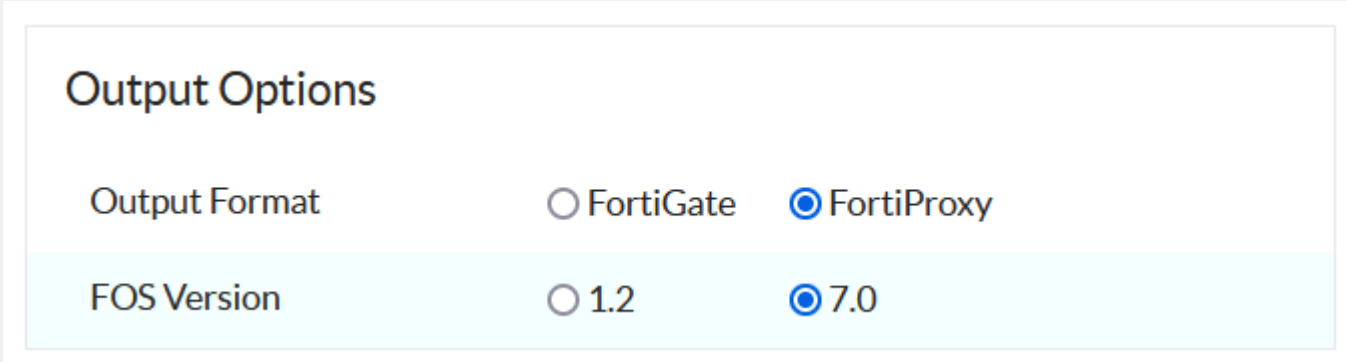
Review the current Policy

Check for correct implementation

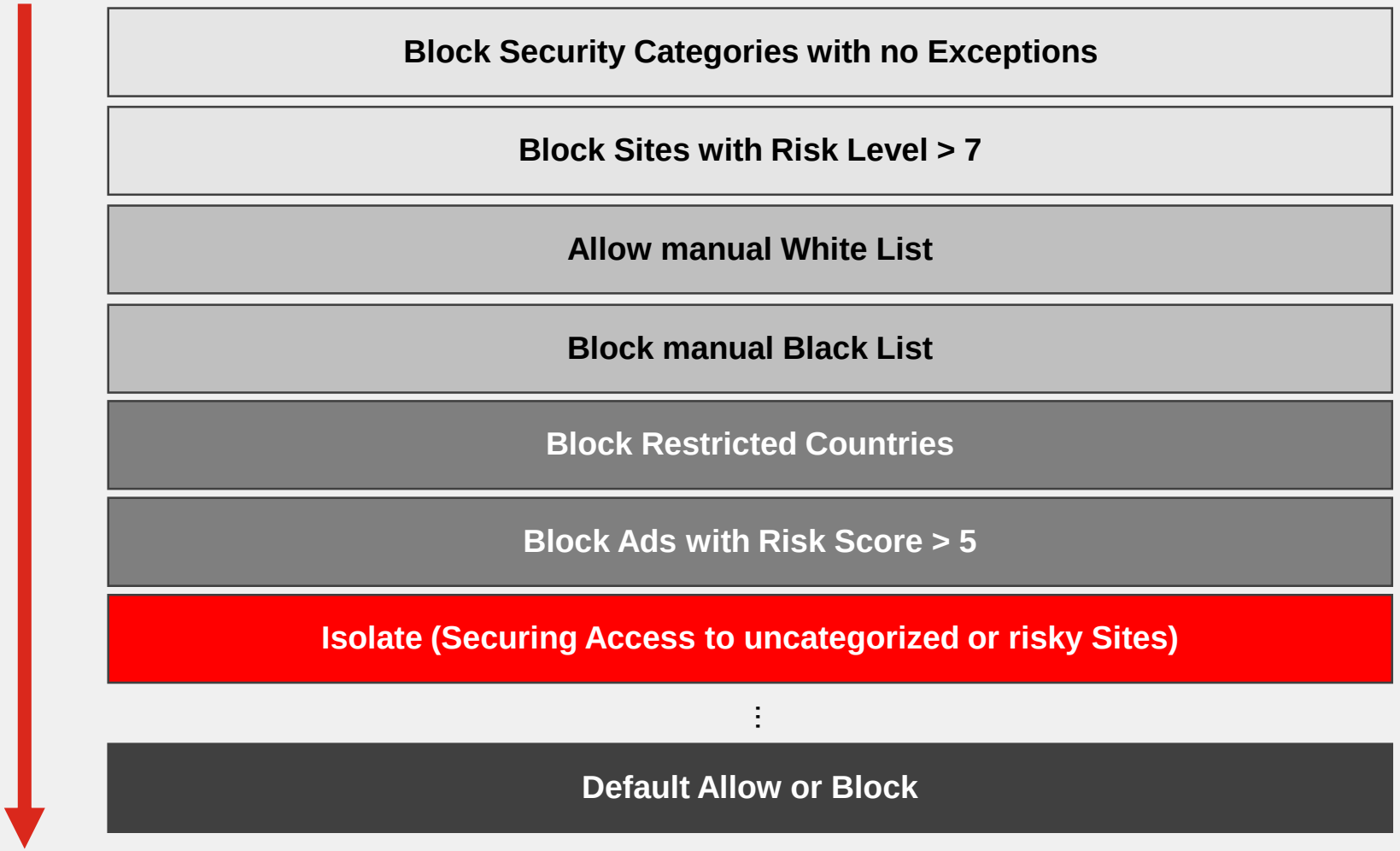
Use Partner Services for Policy migration

Proxy Policy – Migration with FortiConverter





Proxy Policy - with Browser Isolation



Key Message:

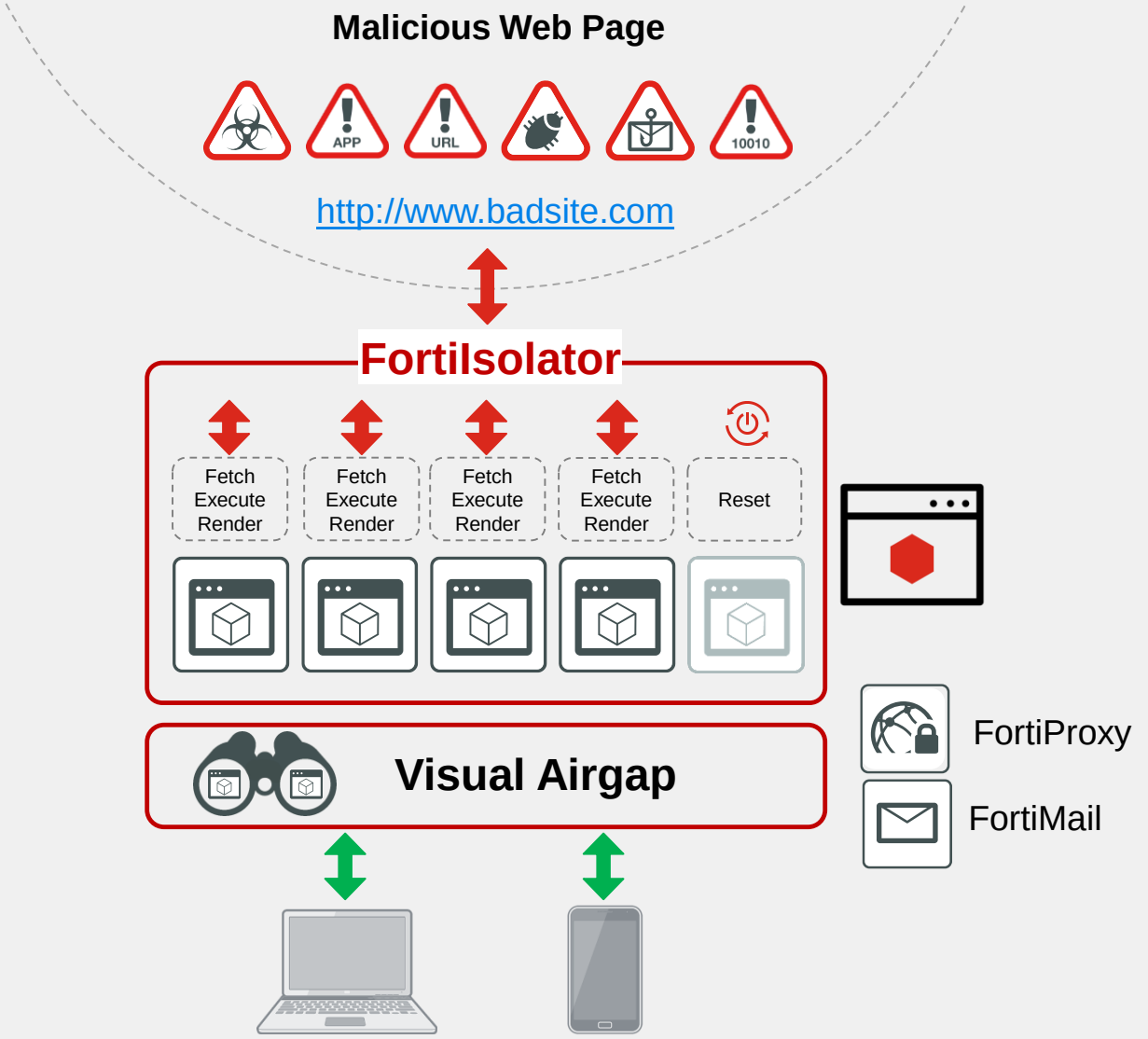
Stop Overblocking

Don’t isolate everything

Expand Internet Browsing experience with zero Malware risk

Introducing FortiIsolator for Zero Trust Web Browsing

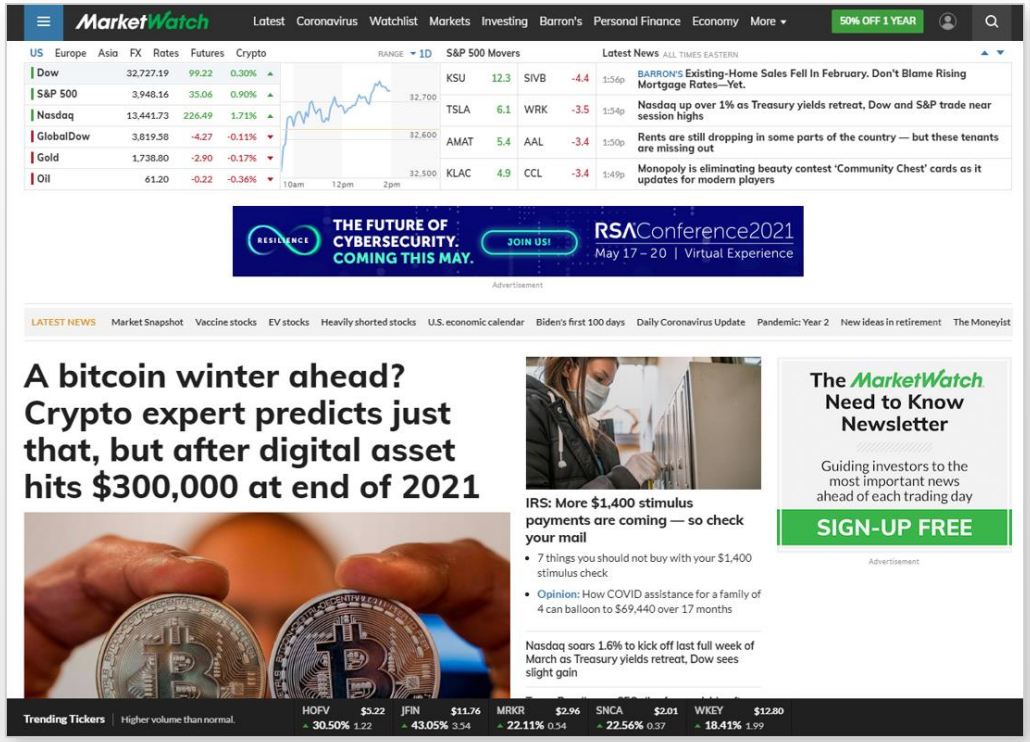
- Clientless remote browser isolation
- Works with any modern HTML5 capable browser
- No third party code ever runs on the local machine
- Browser session runs in clean remote container
- Rendered page image displayed to client
- Supports web page interactivity e.g. links, forms, video, audio



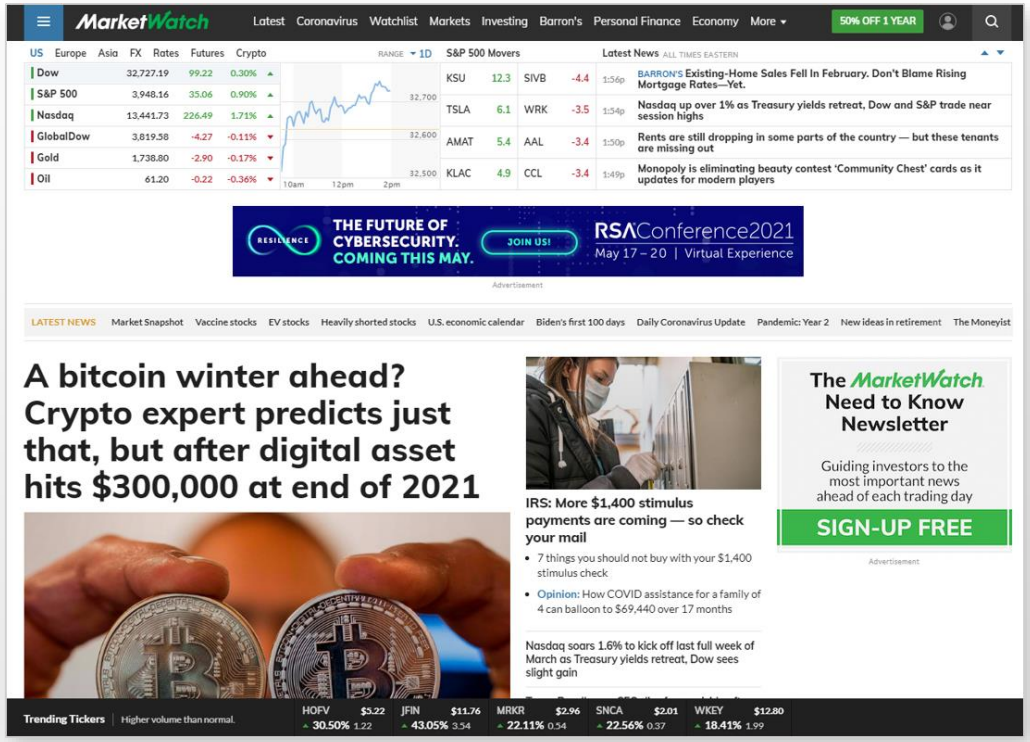
FortiIsolator - Safe Content Rendering

Allows users to browse the web in an isolated environment, which renders safe content in a remote container.

Directly accessed using Browser



Accessed via FortiIsolator using Browser



Safe Content Rendering

Directly accessed using Chrome

20+ Scripts

3rd party scripts & content from iFrame

Tracking cookies & scripts

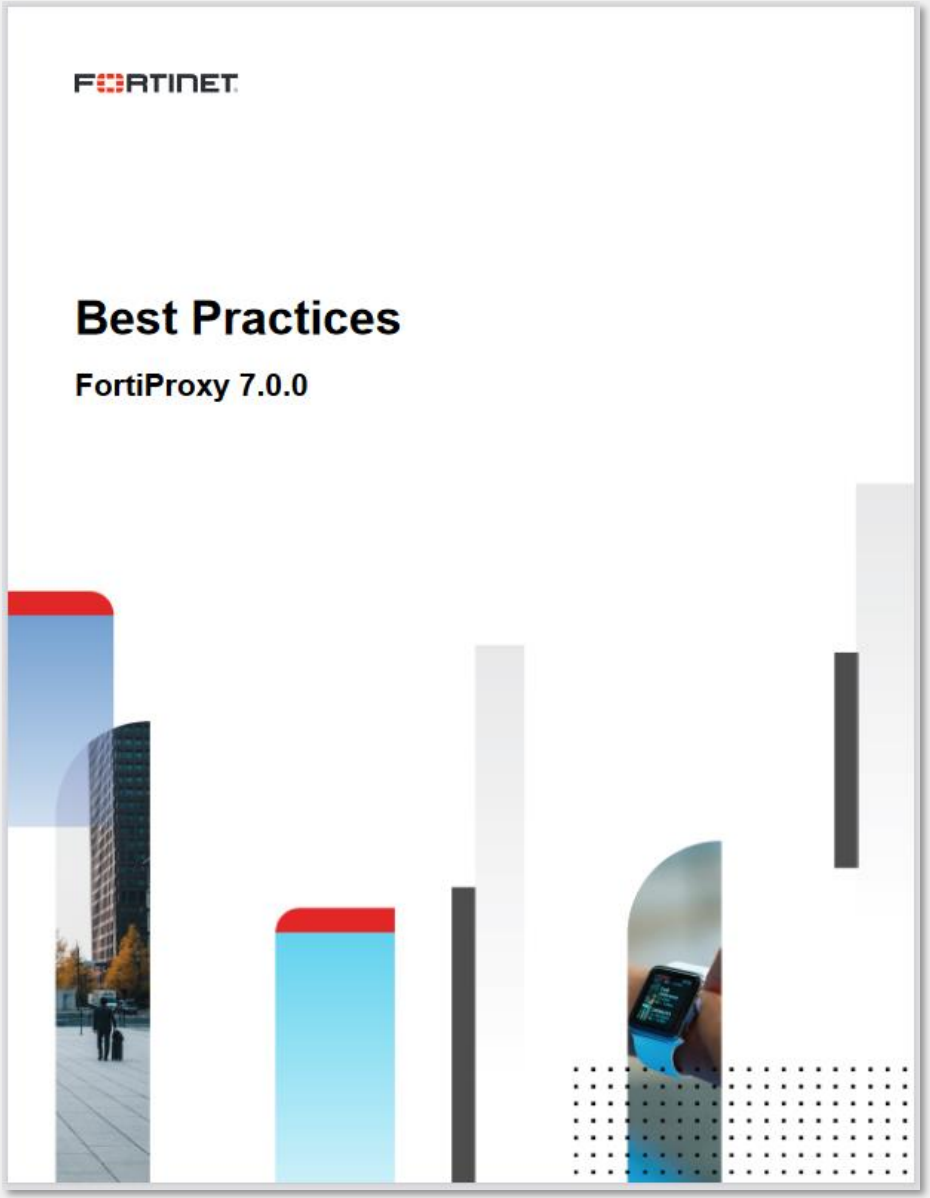
Accessed via FortiIsolator using Chrome

2 FortiIsolator Scripts

```
<!doctype html>
<html style="overflow: hidden;">
▼<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width">
    <link rel="stylesheet" href="https://10.1.0.1:8887/ftnt.css">
    <script src="https://10.1.0.1:8887/jquery.js"></script>
    <script src="https://10.1.0.1:8887/ftnt.js"></script>
    <title>Yahoo</title>
  </head>
▼<body>
... ▶<script>…</script> == $0
    <div id="statusDiv" hidden="hidden"></div>
    <canvas id="mainCanvas" width="150" height="979" style="cursor: default;">
    <canvas id="popupCanvas">
  </body>
</html>
```

Objectless

FortiProxy Best Practices



Training & Licensing

FortiProxy License Offering

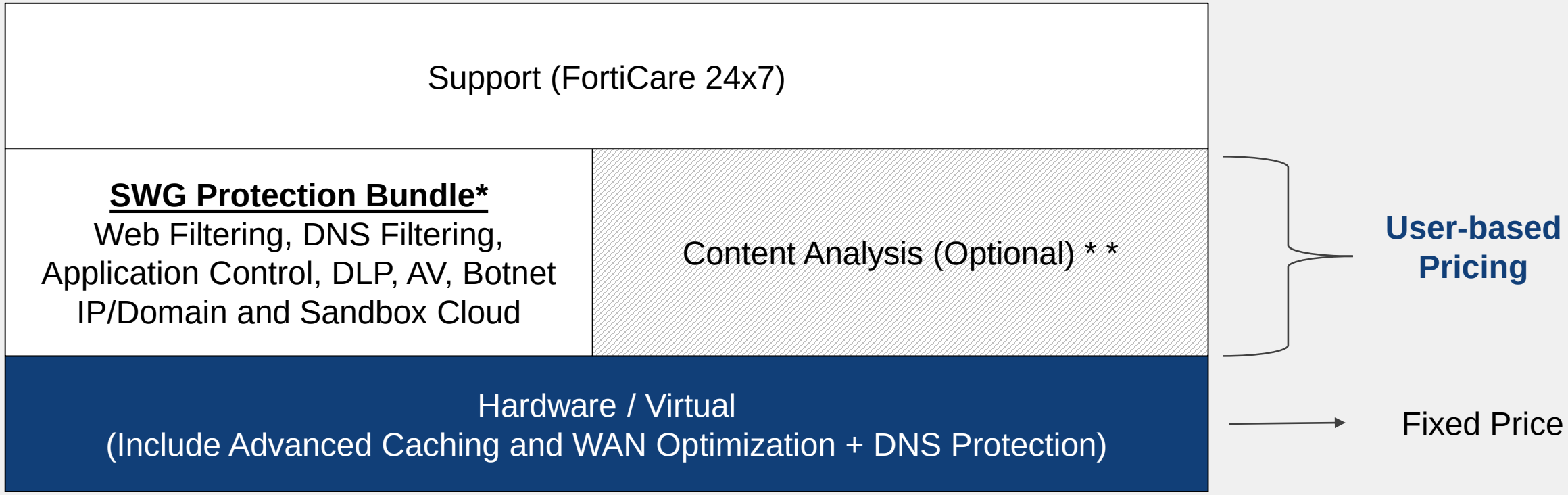
FortiProxy offers **PAYG** License (per “seat/user”) which allows the customer to scale according to his needs.

Benefits:

- Scalable performance without the need for hardware replacement
- Customers pay only for the exact capacity currently required, which prevents over-spending on the initial solution
- Overcomes capacity planning challenges
- Reduces the risk associated with data center growth for best investment protection

Licensing Model

***PAYG** User Based Licensing – Minimum users required*



* Scale up to 50K users depend on HW/VM Model

* * Equal to SWG Protection Bundle amount

Documentation

https://docs.fortinet.com/product/fortiproxy/7.2

Admin Guides

Administration Guide
7.2.0
Last updated Oct. 24, 2022

Virtualization
7.2.0
Last updated Sep. 16, 2022

Cloud Deployment Guide
7.2.0
- FortiProxy Public Cloud
- FortiProxy Private Cloud

Reference Manuals

Command Line Interface (CLI)
7.2.1
Last updated Oct. 18, 2022

UTM Packet Flow
7.2.0
Last updated Sep. 16, 2022

Maximum Values
7.2.0
Last updated Sep. 16, 2022

Supported RFCs
7.2.0
Last updated Sep. 16, 2022

FortiProxy Ports
7.2.0
Last updated Sep. 16, 2022

REST API
7.2.0
Last updated Sep. 16, 2022

Fast Track Training

[Security Driven Networking] Protecting and Accelerating User Web Access

In this workshop, participants will learn how to protect and accelerate user web access.

This session covers:

- Set up an explicit web proxy (FortiProxy)
- Set up network settings on browser to point to FortiProxy
- Accelerate the Web Access, Protect against Visual Threats, YouTube Filtering
- Browser isolation and integration with proxy (FortiIsolator)

Fast Track Summary

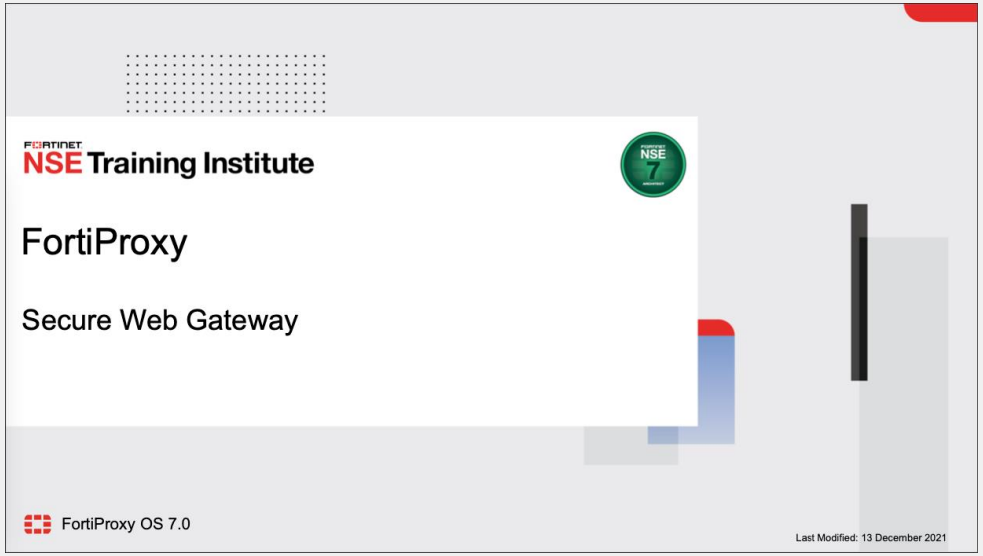
In today's networks, HTTPS/SSL Traffic percentage has increased dramatically along with number of social websites, risky content on the internet and attacks. This increase brings the need of protection from internet born threat, drive growth of web security market and the need of acceleration of Web Traffic.

FortiProxy is a secure web proxy that protects employees against internet-borne attacks by incorporating multiple detection techniques such as web filtering, DNS filtering, data loss prevention, antivirus, intrusion prevention, and advanced threat protection. It helps enterprises enforce internet compliance using granular application control. Content Analysis Enforce acceptable usage by detecting and preventing illicit images and videos with AI-driven content analysis

FortiProxy has a powerful hardware that can perform SSL inspection to effectively remove blind spots in encrypted traffic, without compromising on performance. FortiProxy uses specialized ASICs to accelerate performance of the network and security modules. FortiProxy supports proxy speeds up to 15 Gbps and can scale from small enterprises with 500 users all the way to larger enterprises of 50,000 users.

NSE Training

- Work in progress on fast-track and NSE7 with training team
- The curriculum development managers responsible for managing NSE Institute training courses are in the planning stages of creating a new NSE course for FortiProxy
- INTL CSE team is heavily involve in reviewing the course contents

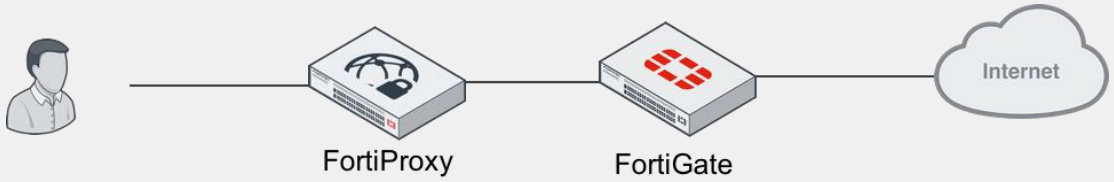


Q&A

Thank you!

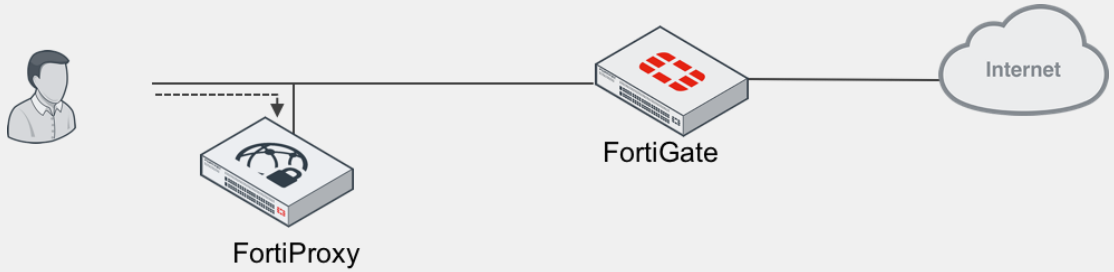
Deployment Modes

Inline (L2/L3) Deployment



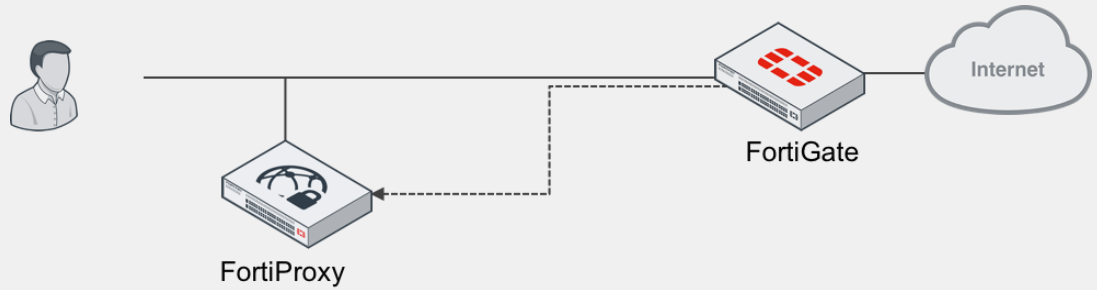
- FortiProxy appliance acts as a transparent bridge in the network and analyze client content traversing the device

Explicit Deployment



- FortiProxy acts as an explicit proxy for clients in the network.
- Client browsers must be configured to redirect traffic to the FortiProxy. Supports PAC files.

Transparent/WCCP Deployment



- FortiProxy appliance acts as a transparent bridge in the network and analyze client content traversing the device.
- WCCP can be used to integrate with an existing network architecture and deliver scalability and load balancing. Supports WCCP client and Mask assignment.

FortiProxy v7 – What's new?

FortiManager to bridge the gap

THE solution is FortiManager

Can be used as of FPX v7 for external communication like:

- License validation
- FortiGuard updates
- Web Filter request

7.0.3 ↓ Copy Link Download PDF

Feature support

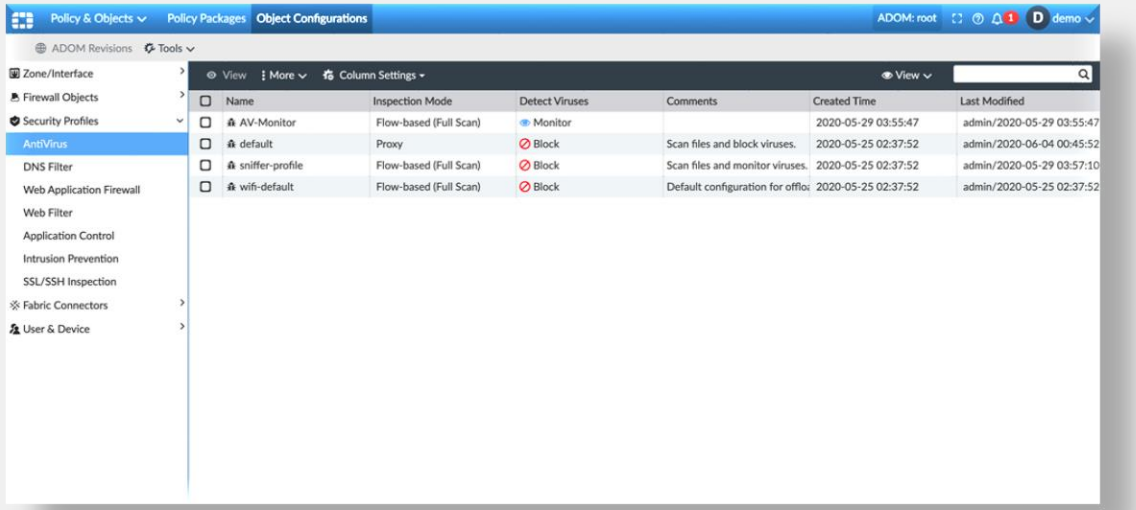
The following table lists FortiManager feature support for managed platforms.

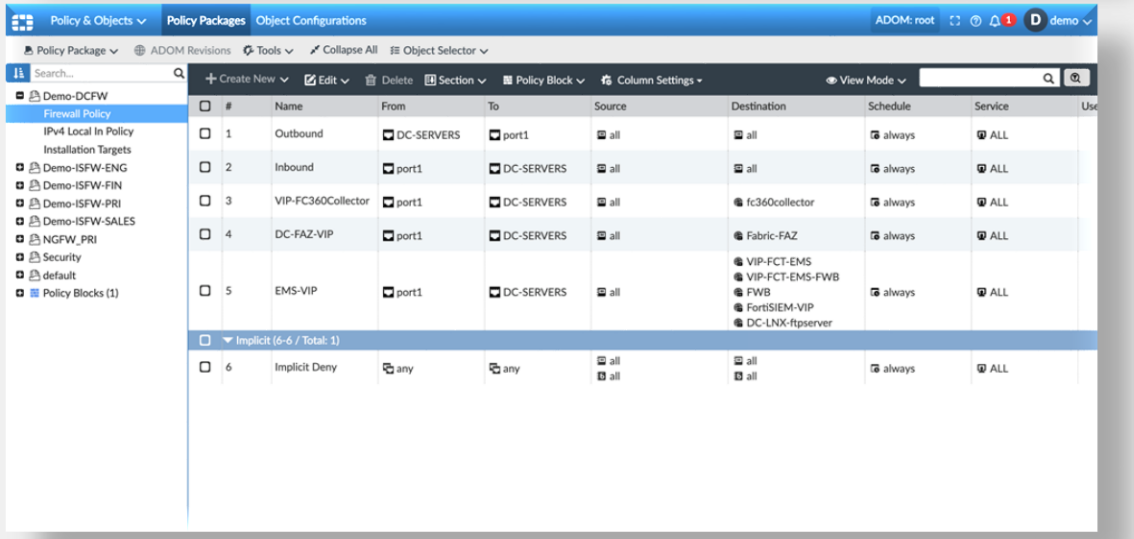
Platform	Management Features	FortiGuard Update Services	VM License Activation	Reports	Logging
FortiGate	✓	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓	✓
FortiADC		✓	✓		
FortiAnalyzer			✓	✓	✓
FortiAuthenticator					✓
FortiCache			✓	✓	✓
FortiClient		✓		✓	✓
FortiDDoS			✓	✓	✓
FortiMail		✓	✓	✓	✓
FortiProxy	✓	✓	✓	✓	✓
FortiSandbox		✓	✓	✓	✓
FortiSOAR		✓	✓		
FortiSwitch ATCA	✓				
FortiTester		✓			
FortiWeb		✓	✓	✓	✓
Syslog					✓

FortiProxy CM – FMG 7.0.3

Centralized Management – FPX v7.0.2 and later

- New FortiProxy ADOM on FortiManager 7.0.3
- Centralized visibility to all FortiProxy, including all sorts of statistics, log, monitoring and licensing
- Services updates from FGD (AV, AppCTRL, ISDB…)
- Global configuration repository, apply to all FortiProxy (v7)
- Global maintenance of all FortiProxy, backup conf, firmware upgrade, etc.





Why the customer requests CM?

None valid use case

- Broadcom/Symantec/Bluecoat do not support Config-Sync Cluster
- CM is needed to help sync the configuration on scalable cluster

FPX can form Config-Sync cluster for scalability purpose without the CM (Natively) !!!

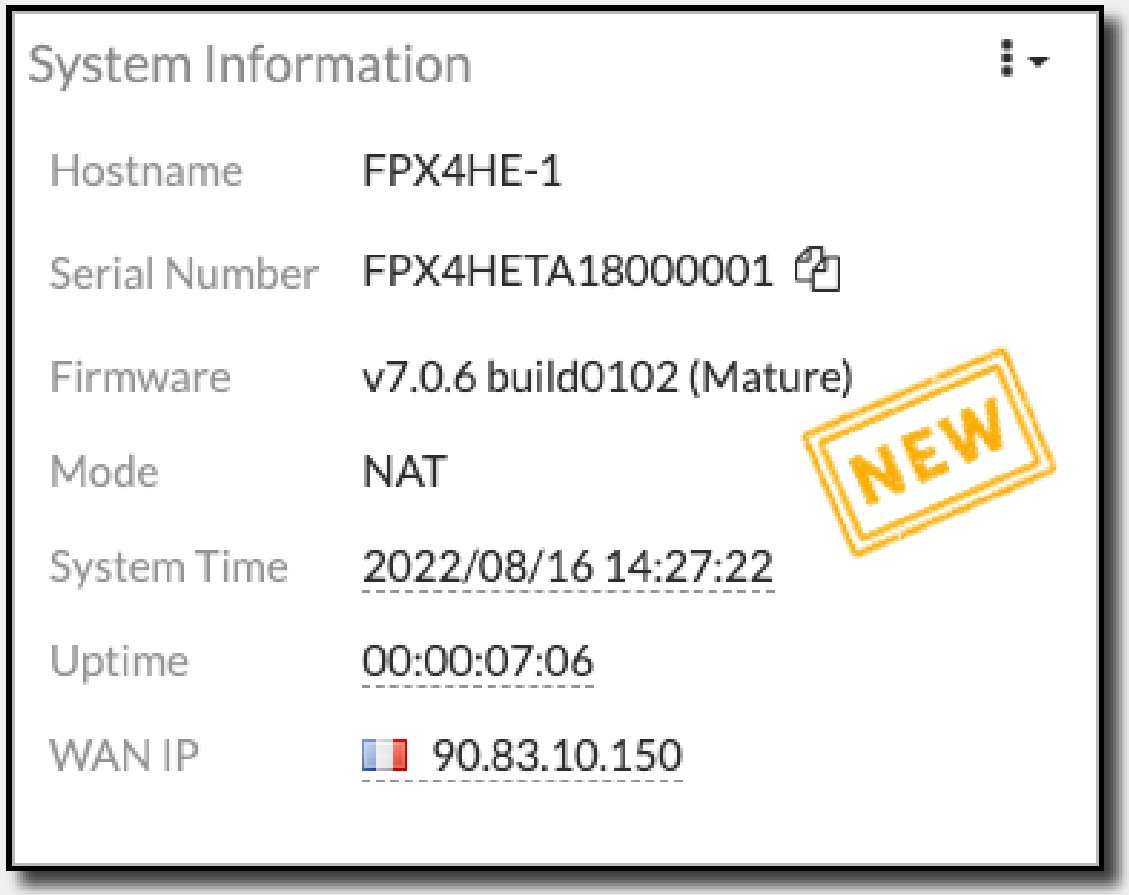
Valid use case

- FPX will need CM to sync the configuration(policy) when we have hybrid environment
- CM will be needed to push same policy set to a mixture of FPX VM and HW
- Policy can be sync between On-Prem FPX and Public Cloud FPX

FortiProxy Software Releases

Select your software release

- “Mature” (v7.0.6 or later)
- “Feature” (v7.2.x)




FORTINET